31 Days Before Your CCENT Certification

Scott Bennett

Cisco Press ▪ 800 East 96th Street ▪ Indianapolis, Indiana 46240 USA

31 Days Before Your CCENT Certification

Scott Bennett

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

First Printing December 2007

Library of Congress Cataloging-in-Publication Number:

Bennett, Scott, CCNA.

31 days before your CCENT certification / Scott Bennett.

p. cm.

ISBN 978-1-58713-217-9 (pbk.)

1. Electronic data processing personnel—Certification. 2. Computer networks—Examinations—Study guides. I. Title. II. Title: Thirty-one days before your CCENT certification.

TK5105.5.B443 2007

004.6076—dc22

2007048436

ISBN-13: 978-1-58713-217-9

ISBN-10: 1-58713-217-6

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Program CCNA Discovery curriculum. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments about how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher	Paul Boger
Associate Publisher	David Dusthimer
Cisco Representative	Anthony Wolfenden
Cisco Press Program Manager	Jeff Brady
Executive Editor	Mary Beth Ray
Managing Editor	Patrick Kanouse
Senior Development Editor	Christopher Cleveland
Senior Project Editor	Tonya Simpson
Copy Editor	Gayle Johnson
Technical Editors	Glenn Tapley, Glenn Wright
Team Coordinator	Vanessa Evans
Book and Cover Designer	Louisa Adair
Composition	Trudy Coler
Indexer	Ken Johnson

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Author

Scott Bennett earned his CCNA, CCAI, and CompTIA A+ while working and teaching in the technology industry. After graduating from Gonzaga University, he went on to work with Qwest eBits, providing network support and training to businesses throughout Idaho. He has four years of experience as a Cisco Networking Academy instructor for the Capital Center High School Technology Institute and Portland Community College. He also wrote *31 Days Before Your CCNA Exam*.

About the Technical Reviewers

Glenn Tapley works as a technical education consultant for Cisco. Glenn has been with Cisco for more than eight years and works on certification courses and exams and is a regular speaker at the annual Networkers and Cisco Live conferences. Prior to Cisco, Glenn was a Certified Cisco Systems instructor for several years with Chesapeake Computer Consultants, Inc., of Annapolis, Maryland. Glenn lives in Florida with his wife and two daughters.

Glenn Wright, CCNA, CCAI, is the codirector of the Cisco Academy Training Center (CATC) in Fort Worth, Texas. He has a bachelor’s degree in business education from the University of North Texas and 22 years of experience in computer education. He has been involved in many aspects of the Cisco Networking Academy since 1999. He serves the Academy as an instructor and supports the Regional Academies in Texas, Louisiana, Oklahoma, Arkansas, North Carolina, South Carolina, Virginia, and Tennessee. He also has worked with the Academy Quality Assurance Team, reviewing and editing Academy curriculum and assessment.

Dedication

To Grandpa Matt; my loving and supportive parents, Jim and Shari; my energetic and caring siblings, Jimmy, Johnny, Monnie, and Christi; and Pam and George for creating my beloved beautiful wife, Angie.

Acknowledgments

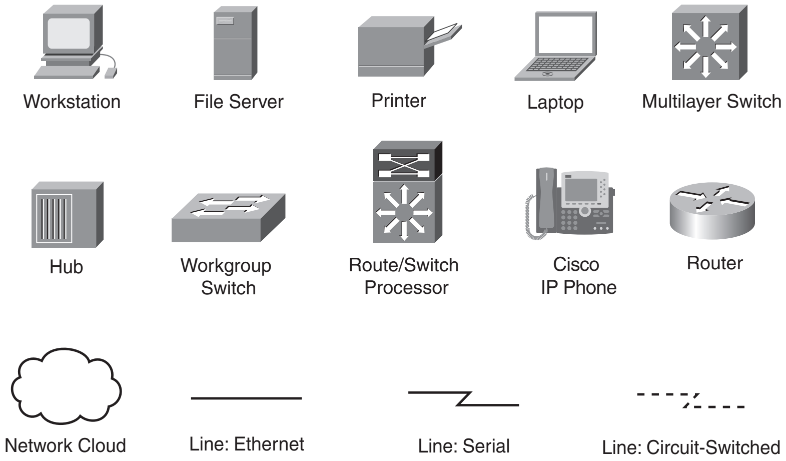
First, I want to thank Mary Beth Ray for her help in this process from start to finish. Her ability to enthusiastically adapt to the ever-changing Cisco certification and Cisco Academy environment amazes me. Thank you for this remarkable experience and opportunity. Thank you to the entire Cisco Press team who worked behind the scenes to help create this book.

I also need to thank Matt Schoenfeldt for his continued and contagious eccentric passion about all things technical. Thanks to Gary Schlienkofer for his work as a regional director and as an instructor for our local Cisco Networking Academy. I also want to thank my friend Peter Buss for providing the perspective and empathy of a seasoned network administrator. Finally, I want to thank Coach Dan Gehn for teaching me the real meaning of the words *endurance* and *dedication*.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.
- A command that does not fit on one line continues on the next line with a two-space indent.

Introduction

31 Days Before Your CCENT Certification represents the end of your adventure through the Cisco Networking Academy CCNA Discovery courses. It's time to pass the ICND1 640-822 exam and make your knowledge official. You owe it to yourself to complete your current Cisco Networking Academy studies with a CCENT certification. This book essentially provides a bridge between the Cisco Networking Academy curriculum and the CCENT (ICND1) exam. Each day breaks down each exam topic into a manageable bite using short summaries from the online curriculum. Use this book and its organized course of study to take the guesswork out of your comprehensive Networking Academy review for the CCENT.

Goals and Methods

The main goal of this book is to provide you with a clear map from the Cisco Networking Academy online curriculum to the CCENT (ICND1) exam. You will read short summaries of sections from the Networking Academy online curriculum as they relate to each of the exam topics for the CCENT. This book also outlines the format of the CCENT exam and the registration requirements you must fulfill to take the CCENT (ICND1) exam.

Each day in this book uses the following elements to review the Cisco Networking Academy online curriculum:

- Short summaries of key concepts and definitions from the curriculum, with a reference to the Networking Academy online module section number.
- Tables and figures to help you recognize topics that you covered during your Networking Academy studies.
- No-frills Cisco IOS Software command-line examples to jog your memory about the configurations and lab exercises that relate to each CCENT objective.
- References for further study and practice testing with the *CCNA Flash Cards and Exam Practice Pack*.
- Brief attempts at networking humor.

This book can also provide instructors and students with a concise way to review the CCNA Discovery curriculum and add a little personality and a new angle to the Networking Academy curriculum. You can use this book to fit CCENT studies into an otherwise busy schedule with a daily timeline and clear references to other CCENT study materials.

Who Should Read This Book?

The primary audience for this book is anyone teaching or enrolled in the Cisco Networking Academy CCNA Discovery courses or recent graduates of the Cisco Networking Academy CCNA Discovery curriculum who have not yet taken or passed the CCENT (ICND1) exam.

The secondary audience for this book is anyone who wants to review for the CCENT, which assumes some prior networking knowledge.

How This Book Is Organized

This book begins with instructions leading you through the process to register for the CCENT exam. Then it breaks up the exam topics by day. The book counts down starting with Day 31 and continues through exam day to provide post-test information. Each day includes subheadings that identify the exam topics that are covered. Each curriculum summary provides the module and section from the corresponding CCNA Discovery course.

You will also find a calendar and checklist that you can tear out and use during your exam preparation. Use the calendar to enter each actual date beside the countdown day, and the day, time, and location of your CCENT exam. The calendar provides a visual for how much time you can dedicate to each CCENT (ICND1) exam objective. You can also put a red X over each day you complete, like those movie montages where the lead character is preparing for something important. Use the checklist to map out your studies leading up to the CCENT (ICND1) exam. The checklist highlights important tasks and deadlines leading up to your exam.

Study Tips

It might help to buy a whiteboard. Get a dry-erase marker and fill the room with that awful scent while you diagram and teach yourself each concept. Teach out loud. Teach whoever will listen. Most important, you need to inject yourself into this information. Your desire to get a CCENT and understand these concepts will shine through on test day. If you cannot explain and diagram an objective, you do not know it. The real test happens when your boss asks you to explain a networking concept or to defend your suggestion in a meeting. The following activities can also help you prepare:

- Podcast audio discussions about CCENT topics.
- Capture video lessons of yourself, and watch them or place them online for others.
- For every hour that you study, donate a set amount to a children's hospital. Ask friends to sponsor you.
- Blog what you are learning.
- Get a copy of *CCNA Flash Cards and Exam Practice Pack*, and tackle the suggested readings and practice exams for each day.

Getting to Know the CCENT (ICND1 640-822) Exam

The CCENT ICND1 640-822 exam tests your ability to describe, implement, configure, secure, and troubleshoot small networks. Just knowing the information will help you on the exam, but also knowing the testing process, format, and testing environment will build your confidence and reduce the chance of any unpleasant surprises on exam day.

Exam Topics

The topics of the CCENT (ICND1 640-822) exam focus on the following seven key categories:

- **Describe network operation:** The topics in this category relate to the theory and concepts behind networks, including layered models, protocols, and topologies.
- **Implement a switched network:** This category asks you to connect, configure, and secure a switched network.
- **Implement an IP addressing scheme:** This category asks you to describe subnetting, NAT, DHCP, DNS, and IP addressing-related tasks on a network.
- **Implement a routed network:** This category asks you to connect, configure, and secure a router on a network.
- **Explain and select administrative tasks for a WLAN:** This category is where you prove that you understand the different WLAN standards and necessary parameters to configure on a WLAN.
- **Identify and mitigate security threats:** This category asks you to describe common network vulnerabilities and how to protect your users and data.
- **Implement and verify WAN links:** This category asks you to describe WAN connections and configure a basic WAN serial connection.

Each category includes general exam topics. In this book, similar CCENT (ICND1) exam topics are grouped into a single day and are explained using the information you have learned in the CCNA Discovery courses.

Although Cisco outlines general exam topics, it is possible that not all topics will appear on the CCENT (ICND1) exam and that topics that are not specifically listed may appear on the exam. The exam topics provided by Cisco and included in this book are a general framework for exam preparation. Be sure to check Cisco.com and look at the latest exam topics. You can navigate to CCENT information through the Training and Events link.

Exam Format

For the CCENT (ICND1) exam, you are allowed 90 minutes to answer 50 to 60 questions**.** Table I-1 outlines each type of question that you might encounter on the exam.

Table I-1 Cisco Exam Question Types

Question Type	Description
Multiple-choice single-answer	You choose one and only one answer.
Multiple-choice multiple-answer you how many answers you must select.	You choose more than one answer. The question tells
Drag-and-drop	You drag and release objects to visually arrange the answer on the page. These questions are similar to the drag-and-drop Interactive Media Activities in the Academy online curriculum.
Fill-in-the-blank	You click a text box and then enter the answer. Sometimes there is more than one text box.
Testlet	You see an upper pane and lower pane in the main win dow for this type of task. The upper pane contains a scenario, and the lower pane contains multiple-choice questions with single and multiple answers. On the right side you can scroll through the scenario and select questions.
Simlet	A top pane contains questions, and a bottom pane contains a router simulation that you can use to answer the questions.
Simulations	This task is similar to the e-Labs that cover configurations. Remember that not all commands are supported in these simulations and that you can view the network topology in some simulations. You see the actual problem at the top and the directions on the left.

Cisco.com has an exam tutorial that simulates each of these types of questions. As you work through the exam tutorial, identify the question types that will take you longer to complete so that you can manage your time on exam day. The following steps allow you to access this tutorial:

Step 1 Visit http://www.vue.com/cisco.

Step 2 Scroll down and visit the link labeled Review the Cisco Certification Exam Tutorial.

Step 3 Click the Certification Exam Tutorial link.

ICND1 640-822 Discount Voucher

As a Cisco Networking Academy student, you have a unique opportunity to integrate your final days of study with preparation for the CCENT exam**.** Before you complete the CCNA Discovery 2 course (Working at a Small-to-Medium Business or ISP), you should plan to pass the final exam with a 75% or higher **on the first attempt.** If you do so, you can request a discount voucher for the ICND1 exam on your Cisco Networking Academy home page. It is important to schedule the CCNA Discovery 2 final so that you have time to properly prepare and achieve a 75% or higher on your first attempt. Work with your instructor to choose an optimal time and environment to take the final.

Registering for the CCENT (ICND1 640-822) Exam

After you have taken the final and redeemed your voucher, you need to gather the information outlined in Table I-2 to register for the ICND 640-822 exam.

Table I-2 Personal Information for ICND 640-822 Exam Registration

Item	Notes
Legal name	
Social security or passport number	
Cisco certification ID or test ID	
Cisco Academy username	Required for your voucher
Cisco Academy ID number	Required for your voucher
Company name	
Valid e-mail address	
Voucher number	Required for your voucher
Method of payment	Typically a credit card

You can register for an exam up to six weeks in advance or as late as the day before the exam. If you had an account with the Pearson VUE before you began with the Networking Academy, it is important to ensure that your profile is updated with your Academy information for the Academy voucher before you register. You can contact Pearson VUE as shown in Table I-3 to register for an exam. The process and available test times vary based on the local testing center you choose.

Table I-3 Test Delivery Partners

Testing Partner	Phone Number	Website
Pearson VUE	In the U.S. and Canada, call 1-800-829-6387. Choose option 1 and then option 4. Check the website for information for other countries.	http://www.vue.com/cisco

There is no better motivation for study than an actual test date. **Sign up as soon as you have your voucher.**

Part I

Days 31–27: Describe the operation of data networks

Day 31 covers network components and operation

Day 30 covers layered model applications

Day 29 covers layered model protocols

Day 28 covers network diagrams and topology

Day 27 covers troubleshooting and LAN versus WAN

Day 31

Describe the Purpose and Functions of Various Network Devices

This first exam topic expects you to know the names and general functions of network devices. This is similar to something you might tell your friend at lunch if he or she asked for a 5-minute explanation of the computer lab at the library. As soon as you know the names of the devices, Days 30 and 29 look at their language (protocols). Chapters 1 and 3 of *CCNA Discovery 1* describe network devices and their functions.

CCNA Discovery 1, Chapter 1

1.1.1 and 1.2.1: Computers exist in numerous environments: businesses, homes, schools, cars, cell phones. Most computers consist of hardware, an operating system, and application software. You would purchase a desktop or laptop for your home. However, for your graphic design business, you might choose a beefy workstation. A network administrator may set up an e-mail server and carry a handheld for alerts and remote network access. A large business might purchase a mainframe to handle special enterprise tasks.

1.2.2 and 1.2.3: The following hosts are often attached to a network:

- **Servers** provide application services to client computers. Servers typically have multiple hard drives and increased processing power and memory. Servers provide services such as file storage, web page hosting, e-mail storage, and print services. Although it is always connected to a network, a server may not have a keyboard, monitor, or mouse connected.
- A **desktop** uses a mouse, keyboard, and monitor to give the user direct access to local applications such as word processing and network applications such as e-mail.
- A **workstation** is a customized desktop designed for a specific application that demands improved hardware such as dual monitors, a specialized 3-D card, a faster disk drive and processor, or increased memory.
- **Laptops and handheld computers** provide more accessible mobile devices with relatively less powerful hardware than desktops or workstations. Portable devices are also more difficult to upgrade.

1.4.1–1.4.3: A preassembled computer system can cost less, but it might not have the performance level of a custom-built computer system. The main components of a computer are the motherboard, central processing unit (CPU), and random-access memory (RAM). A computer system that has no built-in or compatible network connection may require a network interface card (NIC) to communicate on the network. As with any adapter card, the NIC typically attaches to the motherboard.

CCNA Discovery 1, Chapter 3

3.1.1 and 3.1.2: Earlier networks provided only a single dedicated and specific service, such as voice communication. The structure of each dedicated network allowed voice communication or video transfer, but not both. Today, newer converged networks can offer voice, video, and data from a single device over the same network. Devices connected to a network allow users to communicate electronically, share resources, and engage in online trade. The Internet is an example of a converged network capable of simultaneous voice, video, and data transmission.

3.3.5: One way to classify the purpose and placement of networking devices is through a hierarchical model. We will revisit network design models on Days 29 and 28. The following points outline a three-layer hierarchical model:

- **Access layer devices** connect hosts on a local-area network (LAN).
- **Distribution layer devices** provide connectivity between LANs.
- **Core layer devices** provide high-speed connectivity between distribution layer devices.

3.4.2, 3.4.3, and 3.5.2: In addition to hosts, networks include hubs, switches, and routers. Table 31-1 describes the purpose of each of these networking devices.

Table 31-1 Networking Devices and Their Purpose

Device	Layer	Purpose
Hub	Typically installed in a LAN at the access layer	Ethernet networking device with multiple ports that simply regenerates a signal it receives on one port to all other ports. All devices are on the same channel and share that channel's bandwidth. If two devices send a message at the same time, a collision occurs.
Switch	Used at the access layer	Multiport networking device that looks at the destination physical address of a received frame on one port to forward the frame to the port where the host is connected. Hosts communicate through temporary circuits, avoiding collisions. A bridge is essentially a two-port switch an administrator could use to divide a large, hub-based collision domain. Recent network installations implement switches rather than hubs and a bridge.
Router	Connected at the distribution layer	Routers look at the destination IP address of a received packet and forward the packet to its destination network. Routers also determine the best path for a packet to its destination network.

Select the Components Required to Meet a Given Network Specification

As soon as you understand the devices and their functions on a network, selecting the proper components becomes easier. Chapter 3 of *CCNA Discovery 1* provides an overview of the components necessary to build a network.

CCNA Discovery 1, Chapter 3

3.1.3 and 3.1.4: To create a network, you first set up hosts and connect peripherals to them. An example is a desktop with a scanner attached. Next you use some form of media to connect the hosts to a hub or switch. Other users can now share the peripheral devices over the network. To attach your local network to other networks, you connect a router. In addition, hosts can act as servers if you install specific software that enables the host to provide information. Just as a web server requires your computer to have a web browser, many network server applications require a client to run specific software.

Summary

The information covered today provides a brief overview of the key components of a network. When you sit in front of a desktop to send an e-mail, your transmission passes through physical media, then to a hub or switch, then to a router, and lastly to a server, where it sits until requested by the recipient. Days 30 and 29 describe the software and protocols used by these networking devices to transmit, forward, and route this information. If you have a copy of the *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition, you can further review the topics from today on pages 5–36.

Your Notes

Day 30

Use the OSI and TCP/IP Models and Their Associated Protocols to Explain How Data Flows in a Network

A layered model provides the foundation for your understanding of networks. The stronger you build this foundation, the more information you will be able to easily learn and retain. When you learn, teach, troubleshoot, and tackle network configuration, the Open Systems Interconnection (OSI) model and the Transmission Control Protocol/Internet Protocol (TCP/IP) model should guide your plan of attack. Not surprisingly, the CCENT exam tests your ability to describe networks using a layered model. This section includes topics covered in Chapter 6 of *CCNA Discovery 1* and Chapter 2 of *CCNA Discovery 2*.

CCNA Discovery 1, Chapter 6

6.1.1: As defined on Day 31, a host running a server application provides information and services to other hosts running client applications. The communication between a server and client requires a set of standards and protocols.

6.3.1: When hosts communicate over a network, they implement many protocols. This protocol stack is made up of layers, each of which relies on its neighboring layers. The lower-layer protocols focus on moving the data across the network, and the higher-layer protocols focus on the format of the data in the transmission. When you use a layered model to learn network protocols, you can single out the operation of a single layer and how it interacts with other layers. The following list explains the benefits of a layered model:

- Helps with the design of protocols, because each layer has a standard function and a standard interface for communication with adjacent layers.
- Allows products from different vendors to work together, allowing for collaboration in design and competition between manufacturers of compatible components.
- Allows the technology of one layer to improve without affecting other layers.
- Provides common terminology to teach, learn, and discuss networks and network protocols.

The first layered model for internetworking was the Internet or TCP/IP model. This four-layer model consists of the application layer, transport layer, Internet layer, and network access layer. Table 30-1 describes each layer of the TCP/IP model.

Table 30-1 TCP/IP Model and Corresponding Protocol Data Units (PDU)

Layer	Function	PDU
4 (Application)	Deals with network applications.	Data
3 (Transport)	Deals with host-to-host communication.	Segments
2 (Internet)	Deals with the routing or path of the communication.	Packets
1 (Network Access)	Deals with two functions: the framing of the data and signaling over the physical media.	Frames, bits

6.3.2: The following steps take you through the flow of data through a network using the TCP/IP model protocol stack as a reference:

1. You start at the top of the protocol stack with the application layer. For example, you use a network application such as a web browser to make a Hypertext Transfer Protocol (HTTP) request for a web page.

2. At the transport layer, the request is broken down and encapsulated into a Transmission Control Protocol (TCP) **segment** and is given a header identifying the source port, destination port, and sequence number. Some applications at the transport layer use the faster, less reliable User Datagram Protocol (UDP).

3. At the Internet layer, the TCP segments are encapsulated into Internet Protocol (IP) **packets** and are given an IP header with a source and destination IP address.

4. The network access layer uses the Ethernet protocol to encapsulate the packets into frames. Each frame has a header including a source and destination media access control (MAC) address, as well as a cyclical redundancy check (CRC) field at the end of the frame to verify proper transmission. In this layer, the frames are also encoded into bits and are sent electronically over the medium by the network interface card (NIC).

5. After the bits cross the physical medium and arrive at the destination, they are de-encapsulated up the protocol stack until the data reaches the application. In this case, the HTTP request would reach the server application, and it would respond with web data and start the process again.

6.3.3: Another reference model for network communication, the OSI model, was created in 1984 by the International Organization for Standardization (ISO). Unlike the TCP/IP model, which focuses on the TCP and IP protocols used on the Internet, the OSI model divides all network communication (not just TCP/IP) into seven layers. The OSI seven-layer model provides the same benefits of standardization and independent compatibility as mentioned previously for the TCP/IP layered model. Table 30-2 describes the OSI model and the associated protocols and PDUs for each layer.

Table 30-2 OSI Seven-Layer Model

Layer Name	Protocols and Examples	PDU
7 (Application)	E-mail, FTP, HTTP	Data
6 (Presentation)	ASCII, .txt, .mp3	Data
5 (Session)	SQL	Data
4 (Transport)	TCP, UDP (port 22, port 80)	Segments
3 (Network)	IP (192.168.1.1)	Packets
2 (Data link)	MAC (00-00-0C-1A-22-3B)	Frames
1 (Physical)	Bits (1010010001010001)	Bits

Table 30-3 shows the headers for an Ethernet frame and the encapsulated headers for an IP packet and TCP segment included in the frame. The table also identifies the OSI layer and protocol related to the headers.

Table 30-3 Encapsulated Headers, Layers, and Protocols

Destination	Source	Destination	Source	Destination	Source
Layer 2	Layer 2	Layer 3	Layer 3	Layer 4	Layer 4
00000C111111	00000C03124A	192.168.1.3	192.168.1.8	22	3345
Ethernet MAC er frame header	Ethernet MAC frame header	IP header	IP header	TCP header	TCP head-

Table 30-4 compares the layers of the OSI model and the TCP/IP model.

Table 30-4 TCP/IP Model Compared to the OSI Model

TCP/IP Model	OSI Model
Application (Layer 4)	Application (Layer 7) Presentation (Layer 6) Session (Layer 5)
Transport (Layer 3)	Transport (Layer 4)
Internet (Layer 2)	Network (Layer 3)
Network access (Layer 1)	Data link (Layer 2) Physical (Layer 1)

CCNA Discovery 2, Chapter 2

2.2.1 and 2.2.2: The OSI model is often described in terms of the upper and lower layers. The upper layers include Layers 5, 6, and 7, and the lower layers include Layers 1, 2, 3, and 4. The upper layers deal with the data's format, organization, and communication. The lower layers primarily implement protocols to transport and route data across a network. Table 30-5 outlines the function of each layer and associated network devices.

Table 30-5 OSI Model Functions and Associated Devices

Layer	Function	Devices
7	Software applications that provide services such as Domain Name System (DNS), File Transfer Protocol (FTP), Dynamic Host Configuration Protocol (DHCP), Simple Network Management Protocol (SNMP), Telnet, and HTTP.	Host and network software
6	Encrypt and encode (or represent) data in a standard format such as Secure Socket Layer (SSL), American Standard Code for Information Interchange (ASCII), and Multipurpose Internet Mail Extensions (MIME). Shells and redirectors also operate at this layer.	Host and network software
5	Set up and tear down sessions between hosts. Remote Procedure Calls (RPC), NetBIOS, Structured Query Language (SQL) connections, and Application Program Interfaces (API) operate at this layer.	Host and network software
4	Data encoded by the upper layers is broken into segments that receive either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) headers. These protocols deal with the flow of the data and sequence of the segments.	Firewalls video and voice appliances
3	The Layer 4 segments are encapsulated into IP packets. This layer deals with the path selection (routing) of the data over the network. IP version 6 (IPv6) and Network Address Translation (NAT) also operate at this level.	Routers
2	Layer 3 packets are encapsulated into frames with headers using physical Media Access Control (MAC) addresses to identify source and destination. Ethernet, wireless local-area network (WLAN), Asynchronous Transfer Mode (ATM), and Point-to-Point Protocol (PPP) operate at this layer.	Switches and NICs
1	The Layer 2 frames are encoded into bits, represented as electrical signals, light waves, or radio waves, and are transmitted over cables (copper or fiber-optic) or the air (radio waves).	Repeaters hubs, cables, and wireless

Describe Common Networking Applications, Including Web Applications

Networking applications often define a network's purpose and function. A thorough understanding of common networking applications will aid in your efforts to provide the most useful network for a client. This section identifies the common networking applications described in Chapter 1 of *CCNA Discovery 1*.

CCNA Discovery 1, Chapter 1

1.1.2: Types of application software include industry-specific software such as a medical imaging tool, or general-use software such as office and multimedia software. More importantly, applications can be local or networked. A word processor is a local application, and an e-mail client is a network application. A word processor runs directly from the local computer hard drive, whereas an e-mail application requires the local computer to communicate over a network with a remote computer. Table 30-6 provides examples of local applications and network applications.

Table 30-6 Local Applications and Network Applications

Local Applications	Network Applications
Graphic art software	E-mail client software
3D design software	Instant-messaging (IM) software
Word-processing software	Web browser
Spreadsheet software	Web-based tools (such as maps)
Video-editing software	Videoconferencing software

Summary

The seven-layer OSI model and four-layer TCP/IP model provide a map for the processes of formatting, encapsulating, addressing, encoding, and transmitting data over a network. First, a network application creates data for transmission. Next, the data moves through the OSI layers as segments, packets, frames, and finally bits to be transferred over the network. The receiving device rebuilds the data in reverse, and the receiving network application presents the data to the user. Many protocols are implemented during this communication. Day 29 focuses on the protocols used in the OSI and TCP/IP layered models and the impact of some network applications on a network. You can further review the topics from today on pages 5–36 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Describe the Purpose and Basic Operation of the Protocols in the OSI and TCP Models

From the physical standards for speed to the application requirements to request a web page, protocols standardize network communication. Each layer of the OSI and TCP/IP models contains protocols that define communication inside that layer and with neighboring layers. When, how, how much, and how often information can be sent is covered in Chapters 3 and 6 of *CCNA Discovery 1* and Chapter 7 of *CCNA Discovery 2*.

CCNA Discovery 1, Chapter 3

3.2.8 and 3.3.1: Protocols for communicating over a network provide standards for timing, message format, message size, encapsulation, encoding, and message patterns. The most common protocol to manage these standards for a wired local-area network (LAN) is Ethernet.

3.3.2: The Institute of Electrical and Electronic Engineers (IEEE). The IEEE 802.3 Committee develops the standards for Ethernet technologies. The name of an Ethernet standard often identifies its speed, transmission type, and cabling. For example, 100BASE-T is 100 megabits per second (Mbps) baseband transmission over twisted-pair cabling. Table 29-1 lists some common standards for Ethernet.

Table 29-1 Ethernet Standards

Standard	Description
Dix standard	Digital Intel and Xerox standard for 10 Mbps over coaxial cable
IEEE 802.3 10BASE-5	10-Mbps baseband over coaxial cable (thicknet) capable of a 500-meter distance
IEEE 802.3a 10BASE-2	10-Mbps baseband over coaxial cable (thinnet) capable of a 200-meter distance
IEEE 802.3i 10BASE-T	10-Mbps baseband over twisted-pair copper capable of a 100-meter distance
IEEE 802.3j 10BASE-F	10-Mbps baseband over fiber
IEEE 802.3u 100BASE-T	100-Mbps baseband over twisted pair
IEEE 802.3z 1000BASE-X	1 Gigabit per second (Gbps) baseband over fiber
IEEE 802.3an 10G BASE-T	10 Gbps over twisted pair

CCNA Discovery 1, Chapter 6

6.1.2: The protocols at each layer of the OSI model provide guidelines for the functions of that layer. Each of the following protocols operates at a different OSI model layer:

- An example of a protocol used at the application layer is Hypertext Transfer Protocol (HTTP). HTTP governs how a client application requests information and how a server responds.
- At the transport layer, Transmission Control Protocol (TCP) defines how communicating hosts can control the flow of information and acknowledge information received.
- At the network layer, the Internet Protocol (IP) defines how packets should be addressed and routed to their destination.
- At the data link layer, Ethernet is the most common protocol. IP packets are encapsulated into frames and given a physical address for transmission over the network.
- Network interface cards (NIC) use various physical layer standards (depending on the media type) to determine how bits are represented and sent over the medium.

6.1.3: As mentioned previously, network layer IP is concerned with routing the packets, and the transport layer protocols define how to transmit the information. The two most common transport layer protocols are TCP and User Datagram Protocol (UDP):

- TCP breaks a message into a segment, adds a sequence number to each segment, and acknowledges whether a segment has arrived at its destination. If the destination does not acknowledge a segment, the source retransmits the missing portions. File Transfer Protocol (FTP) and HTTP are two application layer protocols that use TCP.
- UDP does not acknowledge or retransmit segments. In fact, application layer protocols that use UDP do so to transfer information without the overhead of acknowledgment and retransmission. Streaming audio, video, and voice over IP (VoIP) use UDP.

6.1.4: Transport layer protocols use ports to identify a service. If a client makes an HTTP request, it typically identifies the destination port as 80. The client also specifies a unique source port (an unregistered port in the 1025 to 65535 range) so that the server can identify the unique conversation. The client uses a destination port, source port, destination IP address, and source IP address to create a socket that identifies the server and service.

6.2.1: The web address (or domain name) that you enter into a browser is translated into an IP address using Domain Name System (DNS). Like an HTTP server responds to port 80 requests, a DNS server responds to requests on port 53. However, if a DNS server does not know the IP for the domain, it forwards the request to another DNS server. If other DNS servers do not have an entry for the domain, the request times out.

6.2.2–6.2.5: Table 29-2 describes communication between web, FTP, e-mail, and instant messaging (IM) clients and servers.

Table 29-2 Client/Server Protocols

Type	Protocols/Ports	Description
Web servers	HTTP/80 HTTPS/443	Clients make a request of a server on port 80 using HTTP, and the server responds with a web page created in Hypertext Markup Language (HTML). Secure requests occur using HTTPS.
FTP servers	FTP/21 FTP/20	An FTP client makes a request of a server on port 21. As soon as the session is open, the server responds with data on port 20.
E-mail servers	SMTP/25 POP3/110 IMAP4/143	A server sends and stores e-mails accessed by an e-mail client. Clients and servers use Simple Mail Transfer Protocol (SMTP) to send e-mails. Servers use Post Office Protocol (POP) to receive and store messages. Servers can also allow an Internet Message Access Protocol (IMAP) client to receive and store messages and keep the messages in the mailbox on the server.
IM servers	Various, depending on vendor	Users can install compatible IM clients and communicate instantly with other users on the same IM network.

CCNA Discovery 2, Chapter 7

7.2.1: Internet service providers (ISP) support many services and applications. These applications use UDP and/or TCP at the transport layer and IP at the network layer. ISP support personnel must be familiar with the TCP/IP protocols to best maintain reliable communication for users. Table 29-3 provides examples and functions of protocols used in the four layers of the TCP/IP model.

Table 29-3 TCP/IP Protocols

TCP/IP Layer	Protocols (Functions)
Application	DNS, DHCP, BOOTP, SMTP, POP, IMAP, FTP, TFTP, HTTP, HTTPS
Transport	UDP, TCP
Internet	IPv4, IPv6, IP (NAT), ARP, ICMP, routing protocols such as RIP, OSPF, EIGRP, and BGP
Network access	PPP, Ethernet

Note that the application, presentation, and session layers of the OSI model define functions in the application layer of the TCP/IP model. In addition, the data link and physical layers of the OSI model are represented by the network access layer of the TCP/IP model. The OSI model contains more defined layers because it is a theoretical guide, whereas the TCP/IP model is based on actual Internet protocols and standards.

7.2.2: As defined previously, TCP uses acknowledgment and retransmission to increase reliability. Because TCP maintains a persistent connection, it is also classified as a connection-oriented protocol. Conversely, UDP is a connectionless protocol that makes a "best-effort" attempt to send the information without acknowledgment or retransmission. UDP suits applications such as Internet radio that can function with short amounts of data loss. TCP works well as a protocol for applications that require all data to arrive in its original condition, such as e-mail and web applications. The reduction in speed that occurs as a result of TCP is a decent trade-off when reliable data transfer is important.

TCP and UDP segments are placed in packets at the network layer for transmission. This process, as mentioned on Day 30, is called *encapsulation*. At the data link layer, the packets are encapsulated into frames and then represented as bits at the physical layer. The encapsulation process occurs in reverse as soon as the bits reach their destination.

TCP requires a three-way handshake to establish a session for communication:

1. The sending host sends a SYN request for a connection. This request also synchronizes the sequence numbers for segment sending between the two hosts.

2. The destination replies with a SYN-ACK message acknowledging the request and synchronization.

3. The sending host responds with an ACK to complete the connection. The hosts can then communicate and send segments reliably.

If any segments are not acknowledged within a specified time, they are retransmitted. These sequenced segments are assembled by the TCP process and delivered to the upper-layer applications for de-encapsulation into data.

7.2.3: Table 29-4 describes the differences between TCP and UDP.

Table 29-4 TCP Versus UDP

TCP	UDP
Connection-oriented protocol	Connectionless protocol
Reliable protocol with acknowledgment, retransmission, flow control, and sequencing	Unreliable; requires reliability to be implemented in other layers if needed
Greater network overhead	Less network overhead
Used for e-mail, FTP, and web applications that require reliable transmission	Used in DNS, SNMP, DHCP, RIP, TFTP, VoIP, online games, video, and audio

7.4.1: Often, ISPs provide to customers application layer services such as HTTP, FTP, SMTP, POP3, and IMAP4. In addition, an ISP can provide secure services such as HTTPS and SFTP. A web server provides HTTP and HTTPS, a file server provides FTP, and a mail server provides POP3 and IMAP4.

7.4.2–7.4.4: When you set up a web server, you can choose to provide web access through HTTP or more secure access through HTTPS. HTTP messages are sent in clear text (which is easily intercepted), whereas HTTPS uses Secure Socket Layer (SSL) to encrypt the data stream. Keep in mind that HTTPS increases the load on a server, so use it only when necessary. A browser accesses your server with a request made when a user enters a Uniform Resource Locator (URL). The URL typically specifies the location of the server and the location of the folder where the information is stored on the server.

HTTP also supports proxy services. You can set up a network device to receive all the HTTP requests on a network and act as a proxy to make the requests to the actual destination. A proxy server provides increased speed through caching, allows you to filter, and provides better security because your hosts do not directly identify themselves to the outside world.

FTP is a two-part process. One part uses a protocol interpreter (PI) to send and receive control information, and the other part uses a data transfer process (DTP) to transfer the files. The PI operates on TCP port 21. Because FTP implements TCP, it is a connection-oriented protocol. However, FTP can operate with active or passive data connections. An active data connection requires the client to open a port, send the information to the server, and receive a connection from the server. Firewalls often do not allow such incoming connections to internal clients. Therefore, a passive connection is more common because the server opens a port (above 1023) and notifies the client, and then waits for the client to make an outgoing connection.

E-mail servers provide a place for users to store, retrieve, and send e-mail. An e-mail client retrieves e-mail from the server and sends e-mail to the server. When an e-mail server receives an e-mail to send, it uses DNS (as a mail exchager [MX] record) to determine the location of the destination e-mail server and then transmits the e-mail. The information in an e-mail address after the @ symbol identifies the server. The e-mail reaches its final destination when the e-mail client of the intended recipient requests it. E-mail clients and servers implement the following protocols:

- E-mail clients use **Simple Mail Transfer Protocol (SMTP)** to send e-mail to their server, and the server in turn uses SMTP to transfer the e-mail to its destination. SMTP requires the proper message format (header and body) and a running SMTP process on both client and server. SMTP operates on TCP port 25. A server makes repeated attempts to transfer an e-mail and then returns the e-mail as undeliverable after a specified period of time.

- **Post Office Protocol version 3 (POP3)** allows an e-mail client to retrieve e-mail on TCP port 110. The messages are downloaded to the client and typically are removed from the server.

- **Internet Message Access Protocol (IMAP4)** allows an e-mail client to retrieve e-mail on port 143. IMAP4 leaves a copy of the e-mail on the server and allows the client to organize the e-mails on the server. The copies of the e-mails on the server allow for a centralized location and backup for all e-mails.

Describe the Impact of Applications (Voice over IP and Video over IP) on a Network

Simply put, video and voice add traffic to your network—lots of traffic. You can improve the performance of these services with powerful, more reliable hardware and some tweaks at the transport layer. This section explains Layer 1 and Layer 4 considerations for voice and video on your network using Chapters 3 and 7 of *CCNA Discovery 2*.

CCNA Discovery 2, Chapter 3

3.3.6: To remain reliable, your network design should take into account the need for backup power and redundant connections. You should also plan your Layer 3 topology by keeping in mind the type of applications you choose. IP phones and cameras require an IP address, so your IP addressing scheme should allow for these devices in addition to your host. Days 20 and 18 further discuss Layer 3 IP addressing and design.

CCNA Discovery 2, Chapter 7

7.1.2: Reliability is measured by the mean time between failures (MTBF) and mean time to repair (MTTR). You can prevent failures and increase your uptime by purchasing redundant hardware that is capable of the services you agree to provide your users. Reliable redundant hardware increases the availability of network services and guarantees the uptime necessary for critical business services such as IP telephony. As an Internet service provider (ISP), you would need to ensure that your equipment and services live up to the promise you make to your clients; this is often called a service level agreement (SLA).

7.2.4: The transport layer protocols TCP and UDP include headers in each segment that can identify the application that is using the session. The transport layer protocols enable simultaneous sessions from different applications. The port numbers in each segment header can identify the type of application; for example, a segment destined for port 80 is likely a request to a web server. TCP and UDP can place these segments in a separate queue for each specific application, based on the port identified, allowing multiple applications to maintain sessions at the same time.

Just as HTTP is typically assigned to port 80, many well-known applications have assignments to well-known ports. The range for these well-known or registered ports is 0 to 1023; applications use these ports as destination ports. However, a client dynamically selects a port as the source of the communication from the port range 1024 to 65535. An example is a web browser that requests a web page. The browser would use port 80 as the destination port (the typical web server port) and would choose a dynamic port in the higher range to list as the source port for return communication. As mentioned previously, the combination of a port and Layer 3 IP address creates a socket. A socket for a web server at the IP address 10.0.0.25 would be 10.0.0.25:80 (port 80 for HTTP). Many newer network devices allow you to watch, measure, filter, and even prioritize traffic based on the port (and application) identified in each segment. A streaming voice or video connection may require higher overhead and a higher priority than applications that can occur in spurts, such as data loaded from a web page.

Summary

Protocols at the application layer define what services you can access on a network. The protocols at the following layers define how, when, where, and how quickly the information can be sent and received. A web page or file can be sent in sporadic spurts over a network, but voice and video require a more steady, reliable, and, frankly, expensive connection. You can further review the topics from today on pages 39–68 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Interpret Network Diagrams

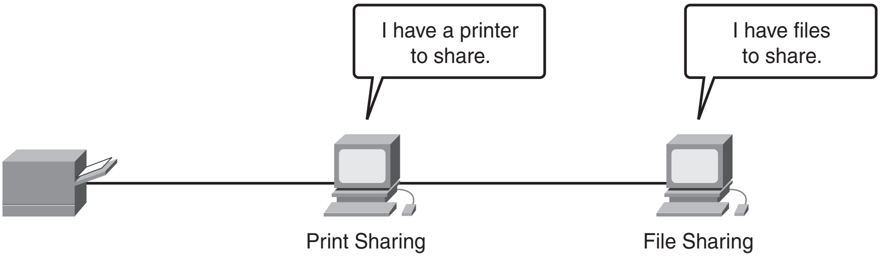
You likely skipped over this book's front matter, which shows all the icons you might encounter in a network diagram. When you connect these icons with special lines, you create network diagrams. The diagrams are meaningless if you cannot understand or explain the theory and concepts they represent. This section explains the structure of the Internet cloud and defines physical and logical topologies using Chapter 3 of *CCNA Discovery 1* and Chapters 1 and 3 of *CCNA Discovery 2*.

CCNA Discovery 1, Chapter 3

3.1.5: As shown in Figure 28-1, a peer-to-peer network can be as simple as two directly connected hosts, or as complicated as multiple hosts connected through various network devices. The key characteristics of a peer-to-peer network are as follows:

- It is decentralized.
- It has no dedicated servers.
- All clients can also provide services such as file and print sharing.

Figure 28-1 Peer-to-Peer Network



The Advantages of Peer-to-Peer Networking:	The Disadvantages of Peer-to-Peer Networking:
• Easy to set up • Less complexity • Lower cost because network devices and dedicated servers might not be required • Can be used for simple tasks such as transferring files and sharing printers	• No centralized administration • Not as secure • Not scalable • All devices may act as both clients and servers, which can slow their performance

3.1.6: When you install a network, you likely start with a detailed map of where the wires and devices should be placed. This physical topology map, shown in Figure 28-2, allows you to locate and troubleshoot devices. In contrast, a logical map of the network topology, shown in Figure 28-3, groups hosts and devices by how they use the network. A logical topology map displays hostnames, address groups, network access, and applications in use on a network.

Figure 28-2 Physical Topology

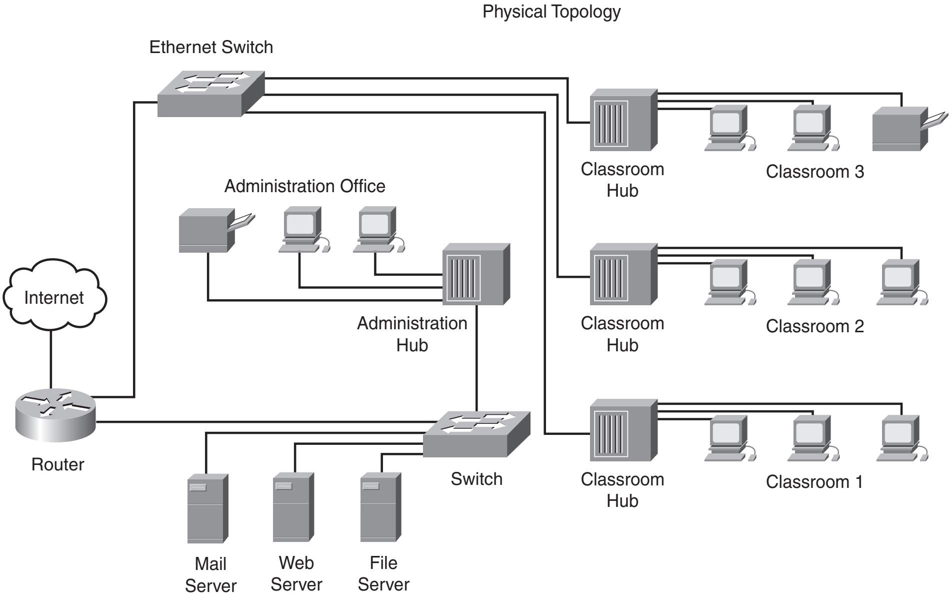
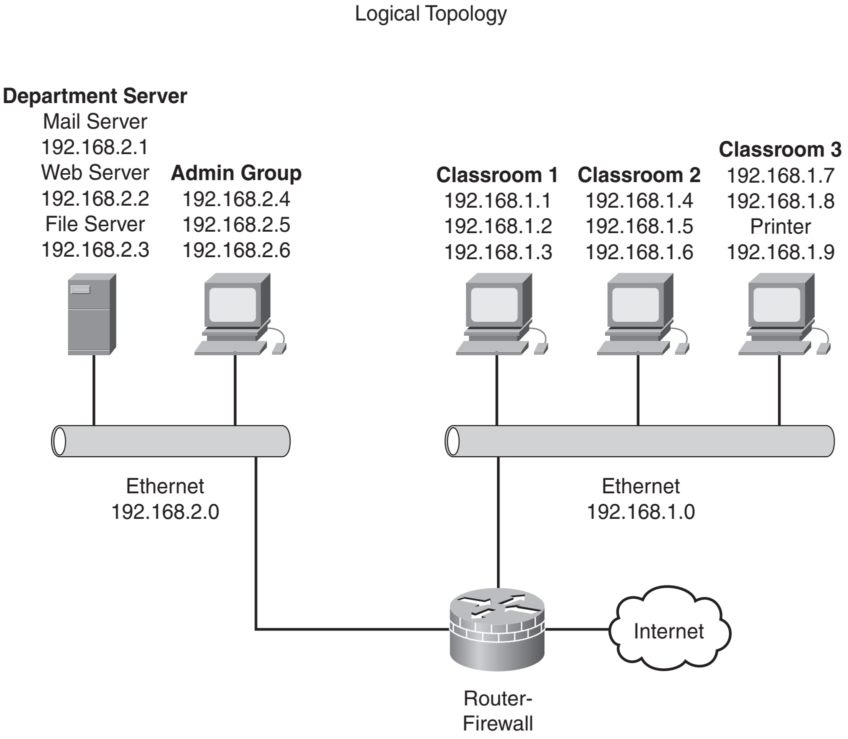


Figure 28-3 Logical Topology



CCNA Discovery 2, Chapter 1

1.2.2: Often the Internet is represented in a diagram as a cloud. This cloud represents the hierarchy of devices that connect you to other networks and the Internet. ISPs sit at the top of this hierarchy and connect to each other through Internet exchange points (IXP) or network access points (NAP). These IXPs and NAPs between ISPs provide the backbone for the Internet. If you want to use the cheesiest term available, refer to these connections as the "information superhighway." This Internet backbone is typically connected with fiber-optic cable installed underground and even undersea. The connections between continents are handled by tier 1 ISPs. The intermediary connections between countries are classified as tier 2 ISPs. Finally, connections between major cities are classified as tier 3 ISPs.

1.2.3: Software applications can aid you in your visualization of connections and speeds possible over the Internet. Entering the following commands in the Cisco command-line interface (CLI) can help you test the connectivity in a network:

- The **ping** command allows you to send an echo request and receive an echo reply to test connectivity. You can also determine the time of the round trip between hosts with a ping.
- The **traceroute** command also allows you to test connectivity between hosts. This command also displays each hop the packet traverses on its trip. A visual traceroute program can provide a diagram of the path the packet travels and the ISPs that forward the information.

CCNA Discovery 2, Chapter 3

3.1.2: To expand on the distinction between a physical and logical topology, a physical topology maps the location of OSI Layer 1 devices and media. A logical topology identifies the Layer 1 devices but focuses on the Layer 3 addressing, access, and upper-layer applications, regardless of location.

Determine the Path Between Two Hosts Across a Network

How does that e-mail or web page get to your computer from the server? Although most people are satisfied with the arrival, you must concern yourself with the trip to pass the CCENT. This section follows the path and protocols involved in data transmission using Chapters 3 and 4 of *CCNA Discovery 1* and Chapter 1 of *CCNA Discovery 2*.

CCNA Discovery 1, Chapter 3

3.3.3: Hosts on Ethernet networks identify themselves with a media access control (MAC) address. When a host communicates over an Ethernet network, it uses its MAC address as the source and the recipient's MAC address as the destination. All hosts on the network that receive the frame compare their MAC address to the destination address and respond if there is a match.

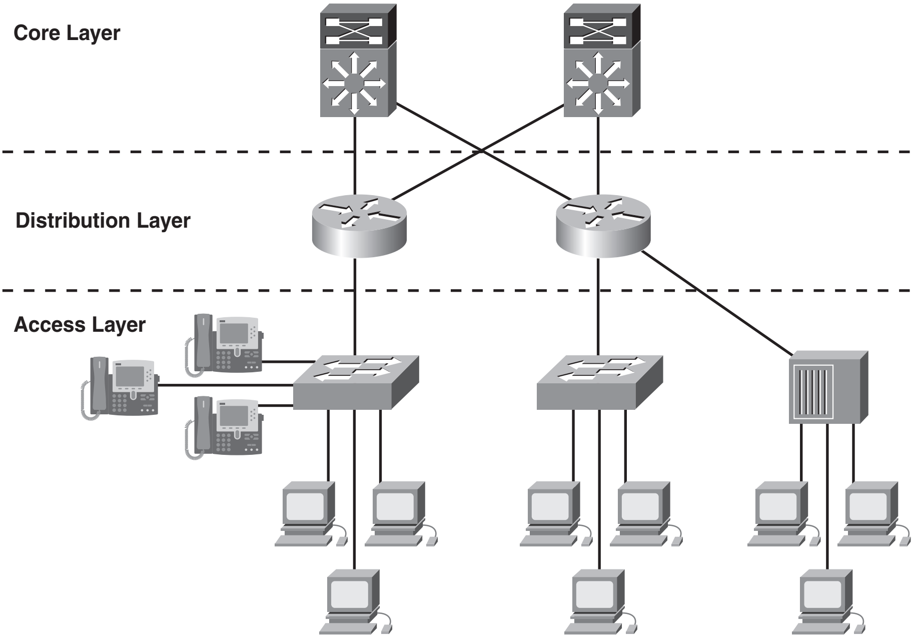
3.3.5: In the hierarchy of the Internet, a MAC address provides a unique identity for a host but does not provide information about the host's location on the network. With millions of hosts on the Internet, it would be unreasonable for each host to look at each communication to decide if it is the recipient. The sending host would have to broadcast its MAC address to all hosts on the Internet, and the recipient would have to broadcast the response. In a hierarchical model, hosts can be divided into small local networks that identify each other by MAC address with routers to communicate between these networks. This model is analogous to the mail system. Each person has a unique name and street address (like a MAC), but the hierarchy of cities, states, and nations better pinpoints the global location to route mail.

In a hierarchical design, local traffic remains local. If a host broadcasts a MAC address destined for a host on the same network, a router doesn't forward the information to other networks. The hierarchical design model can be broken into the following three layers:

- At the **access layer**, hosts connect to each other on the local network.
- At the **distribution layer**, local networks connect to each other.
- At the **core layer**, high-speed devices and media connect distribution layer devices.

Figure 28-4 illustrates the hierarchical design model.

Figure 28-4 Hierarchical Design Model



Whereas a MAC address provides a unique identifier on a local network, an Internet Protocol (IP) address identifies the location of a host in a divided hierarchical network.

3.3.6: A MAC address is physically assigned to the network interface card (NIC) and remains the same on a host. However, the administrator assigns the logical IP address based on the location of the host on the network. An IP address contains two parts: one part identifies the host, and the other part identifies the local network where the host is connected. A host needs both a MAC address and an IP address to communicate over the network.

3.3.7: As mentioned previously, local Ethernet network hosts identify each other by broadcasts and MAC address. A router, however, manages IP traffic. At the access layer, a host is connected to a hub or switch that connects to other hosts on the network. All hosts on this network would have the same network portion of an IP address. At the distribution layer, these networks are connected to routers. The routers forward only IP packets that are destined for other networks. At the core layer, powerful routers and switches move internetwork traffic as efficiently as possible.

CCNA Discovery 1, Chapter 4

4.2.1–4.3.3: To send information over a network, a host provides each packet with a source and destination IP address. Routers use IP to determine whether to forward the packet to another network. The standards for IP are in Request for Comments (RFC) 791.

Each host on the Internet must have a unique IP address. Your IP address likely belongs to an ISP. The ISP received the address (or a block of addresses) from an Internet registry and assigned it to you. When your host sends packets, it places the assigned IP address in the packet header as the source address. The IP packet header also includes a destination address. If the destination IP address is outside of your ISP's local network, the ISP's routers forward it on a path to the outside network. The ISP routers choose the best known path for the destination and forward the packet to other ISP routers. As mentioned previously, you can test connectivity and path selection to a destination with the **ping** and **traceroute** commands. A cloud in network diagrams often represents the numerous routers that choose the path for a packet. Other devices represented by the cloud include DSL Access Multiplexers (DSLAM) and Cable Modem Termination Systems (CMTS); this type of specialized equipment connects the user to the ISP. In addition, the cloud can encompass ISP devices that perform multiple functions, such as an integrated service router (ISR), or enterprise-level high-speed redundant devices to improve reliability and performance.

If the packet is destined for the ISP e-mail server or a local service, it is forwarded to the Network Operations Center (NOC). The NOC controls traffic flow and can provide e-mail, web, or other services, depending on the servers at the facility. ISP devices often perform the same functions as a server and router at a small business; however, an ISP provides these services on a larger scale, with more users and more traffic. ISPs use enterprise-level, high-end equipment, whereas a small business or home office could use smaller, less powerful devices.

CCNA Discovery 2, Chapter 1

1.2.1: The following list defines the connection options for a small office or home user to the Internet:

- Dialup access provides a slower connection through a phone line and a modem. This choice is often driven by a lack of availability of other types of connections, expense, or a lack of teenagers in the household.
- Digital Subscriber Line (DSL) provides a faster-than-dialup, yet more expensive, connection over phone lines. A DSL modem uses a different frequency than a phone, so the user can be on the phone and online at the same time—an optimal configuration for teenagers and small-business users alike.
- A cable modem provides an Internet connection over the same coaxial cable used to provide television.
- A satellite modem can provide connectivity to the nearest ISP using radio signals.
- Dialup typically provides a connection of 56 kilobits per second (kbps). DSL, cable, and satellite can provide 128 kbps and up, depending on the subscriber plan. Typically, for more reliable and/or higher speeds, a business chooses one of the following connections:
  - A T1 can provide up to 1.544 megabits per second (Mbps) for both download and upload. The European standard for a T1 is an E1, which provides 2.048 Mbps.
  - A T3 provides 45 Mbps, and an E3 provides 34.368 Mbps.
  - Businesses can also choose Metro Ethernet if they have multiple branches in a city and need high-bandwidth options such as gigabit-per-second (Gbps) links.

All these users connect to the ISP through a point of presence (POP) on the edge of the ISP's network.

Describe the Components Required for Network and Internet Communications

You typically start with three PCs and a hub or switch on your LAN. Then your friends across town want to e-mail, share files, or play that new online game that your video card barely supports. This section describes the various components you and your ISP could use to network with your friends. Chapters 3 and 4 of *CCNA Discovery 1* and Chapters 1 and 3 of *CCNA Discovery 2* describe common components used in LAN and Internet connections.

CCNA Discovery 1, Chapter 3

3.4.1–3.4.3: Table 28-1 compares the functions of hubs and switches at a network's access layer.

Table 28-1 Functions of Hubs and Switches

Hubs	Switches
A device with multiple ports that simply regenerates a received signal to all ports except the port where the signal is received.	A device with multiple ports that reads each frame's MAC address, maintains a MAC table of which hosts are attached to which port, and forwards frames based on the destination MAC address.
Shared-bandwidth devices see a transmission from one device, and only one device can communicate at a time.	Hosts connected to a switch do not share bandwidth, because the switch creates temporary circuits between communicating hosts based on MAC addressing.
All connected devices are in the same collision domain, because a collision occurs if more than one device sends at the same time.	Multiple conversations can occur without collisions because of the temporary circuits, so each port is its own collision domain on a switch.
If a collision occurs on a hub, it still forwards the frame with errors out all ports. The NICs on the hosts discard the frame.	The switch builds its table from source MAC addresses in frames from sending hosts. If the switch does not yet know a frame's destination MAC address, it floods the frame out all other ports. Switches do not forward frames with errors or frames with the same source and destination.

3.4.4: When a host application intends to send a frame to all other hosts on a network, it sends a broadcast message. Broadcast messages use FFFF.FFFF.FFFF as the destination MAC address. A switch broadcasts this message to all hosts, and all hosts process the message. A network connected with switches and hubs is a single broadcast domain.

3.4.6 and 3.4.7: When an application intends to send information to another host, but it knows only the IP address of the destination, the sending host can use address resolution protocol (ARP).

ARP is an IP protocol that finds a destination MAC when only the destination IP is known. The sending host broadcasts a frame with the IP address. Each host on the network looks for a match with its IP, and the matching host responds with the proper MAC address. If the IP is from another network, the router typically responds with the router's MAC address.

3.5.1: When you design a large network, it makes sense to divide the network into multiple access layer networks. You can divide a network into smaller networks based on the following criteria:

- Physical location
- Logical function
- Security requirements
- Application requirements

Each local-area network (LAN) likely will have hosts connected by hubs and switches. However, distribution layer devices such as routers provide connectivity and communication among LANs.

3.5.2: The following key points define routers:

- Routers connect networks and route packets to their destination networks.
- Routers can look at the MAC address to determine a frame's destination, but routers also decapsulate the frame to look at the destination IP address located in the header of the IP packet.
- Routers look at the network portion of the destination IP address, re-encapsulate the packet, and forward it to its destination.
- Routers maintain a routing table of connected networks. When a router receives a packet, it references the routing table to determine which interface connects to the destination network.
- Routers do not forward frames with a broadcast MAC address, so each port on a router is its own broadcast domain. In other words, routers divide broadcast domains.

3.5.3: On a LAN, hosts with a destination IP address can use ARP requests to find the MAC address of another host. The sending host then pairs the destination MAC and IP addresses in the headers of the outgoing transmission. On the other hand, when a host has a destination IP address that is not on the LAN, it has to use the destination MAC of the router as the default gateway to the remote network. If the router IP address is configured as the default gateway on the host, the sending host can use ARP to find the MAC address of the router. As soon as the host has the MAC address of the default gateway, it can pair the MAC and IP addresses to transmit over the network. The router then receives the transmission, determines the proper interface for the destination network, and replaces the destination MAC address with the MAC address of the next hop.

3.5.4: Routers learn about networks in two ways: when an administrator manually enters a route, or when other routers dynamically report network locations. The router builds a routing table to map networks to its interfaces. In addition, a router maintains an ARP table for local network communication. If a router does not have an entry for a destination network in a packet, the router drops the packet. You can prevent dropped packets by entering a default route. The router forwards all packets with unknown destination networks along the default route. In short, a router uses the routing table to determine the best interface to forward the packet, and then the router uses the

ARP table to get the frame to the next hop with a destination MAC. Each router that forwards a frame specifies a new MAC address for the next hop, but the destination IP address remains the same throughout the transmission.

3.5.5: Although historically a LAN consisted of a single network in a physical location, a LAN can include a number of networks under the same administrative control. These private multilocation LANs are typically called intranets and are connected physically and logically with switches.

CCNA Discovery 1, Chapter 4

4.1.1–4.1.4: LANs and intranets are often owned by businesses or organizations, whereas the Internet as a whole transcends individual ownership. International organizations manage and provide standards for this worldwide connection of networks. ISPs provide the POP for individual user network access through phone lines, cable, or radio waves.

CCNA Discovery 2, Chapter 1

1.3.1: Table 28-2 defines various network-related devices used by an ISP.

Table 28-2 ISP Devices

Device	Description
Digital Subscriber Line Access Multiplexer (DSLAM)	Users connect to the DSLAM with a DSL modem over a phone line for network access.
Cable Modem Termination System (CMTS)	Users connect to the CMTS with a cable modem over coaxial cable.
Dialup modem	Users connect through a modem to the ISP over phone lines.
Wireless bridge	Users connect with a wireless NIC or other wireless equipment over a radio frequency.
Border gateway router	Used by ISPs to connect to other ISPs or enterprise-level customers.
Server	Provides e-mail, file, multimedia, and other network-based services.
Power backup, power and air conditioning	Used by ISPs to maintain steady, reliable power and a controlled environment.

CCNA Discovery 2, Chapter 3

3.1.3: You can identify and track components on a network through proper documentation. A common documented network would include the device name, location, model, operating system, logical address, connection type, and security information.

3.3.1–3.3.5: A business can own its networking equipment or enter into a lease agreement with the ISP to provide and maintain the necessary equipment. When selecting equipment, consider the following points:

- Devices that operate at higher levels of the OSI model can better analyze and forward traffic. Hubs simply repeat binary information, whereas a switch creates temporary circuits using the MAC address and increases collision domains.
- Routers, especially ISRs and Layer 3 switches, have blended functionality.
- Wireless access points can provide more freedom for connectivity, but they must be balanced with security considerations.
- Additional devices such as IP phones or IP cameras may require power over Ethernet or other accommodations in an overall network design.
- ISRs can combine many functions traditionally handled by individual devices: routing, switching, firewall security, and wireless access. In addition, your network may require ISR features such as security, quality of service (QoS), voice over IP (VoIP), Network Address Translation (NAT), and Dynamic Host Configuration Protocol (DHCP).
- Ensure that you can manage and expand your network when choosing the number and type of ports on a router or switch. Consider expansion slots to accommodate future connectivity and port capacity upgrades.
- A branch office with fewer users may function with a Linksys ISR or similar device, whereas a larger branch office may require a medium-sized business router such as the Cisco 1841 ISR. As network host and traffic needs increase, so does the need for bigger, beefier network devices.

Summary

You start with pictures and lines representing devices and cables and end up with a fully functional network running protocols and processing code at the speed of light, or at least the speed of electricity. Some consider network design an art; I like to call it work. Either way, it is important that you understand the topologies a diagram may present on the CCENT, the protocols and path for data across that diagram, and the function of each hop or component that helps the transmission along. Day 27 looks at what to do when problems occur somewhere along the way. You can further review the topics from today on pages 71–84 and 89–112 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 27

Identify and Correct Common Network Problems at Layers 1, 2, 3, and 7 Using a Layered Model Approach

The OSI and TCP/IP models provide an excellent framework for troubleshooting. You can isolate the network issue to a particular layer and test the protocols and configurations for that layer. With a layered model you have a road map for a step-by-step troubleshooting process. Chapters 3 and 9 of *CCNA Discovery 1* and Chapter 2 of *CCNA Discovery 2* discuss troubleshooting.

CCNA Discovery 1, Chapter 9

9.1.1: One key to success in troubleshooting is to use proper documentation. A good troubleshooter might document the problem, the steps taken to determine the cause, and the steps to correct the problem. Detailed documentation of successful and unsuccessful troubleshooting can prove a valuable reference for later situations.

9.1.2: When you encounter a network problem, the first step is to gather information. Ask the individual who reported the problem to identify recent actions and symptoms, refer to any existing documentation about the involved equipment, and use any available network monitoring tools to view logs and recent network activity.

9.1.3: The following points outline possible approaches for a troubleshooting process with a layered concept of networking:

- **Top down:** Start with the application layer, and work down through the layers of the OSI model. This process starts from the perspective of the user and first tests to see if other applications are functioning properly.
- **Bottom up:** Start at the physical layer, and work up the OSI model. Many issues with connectivity are caused by a simple problem with a media connection or power to a device. This is a slow mechanical approach that can take time if the issue is with the application.
- **Divide and conquer:** Experienced troubleshooters often begin at the layer indicated by the symptoms of a particular problem. This can quickly cut to the center of the issue, but it requires advanced understanding and more experience.

In addition to an approach structured around the OSI model, you can troubleshoot through trial and error or substitution. An experienced troubleshooter can figure out the general issue and succeed with a trial-and-error approach. If equipment is available, a troubleshooter can also quickly isolate a problem with substitution. If the error persists, the substituted device is not the problem.

9.2.1: To detect physical layer problems, you can

- Look for damaged or incorrectly connected cables and check indicator lights
- Smell and feel for signs of overheating or improper fan or hardware operation
- Listen for changes in hardware functionality, such as a malfunctioning fan or disk drive

9.2.2: Many commands can assist in Layer 3 and upper-layer troubleshooting. The following commands display information about connectivity and configuration on a device:

- **ipconfig** shows the IP configuration.
- **ping** tests network layer connectivity between devices.
- **tracert** tests connectivity and displays each hop.
- **netstat** shows any network connections to the device.
- **nslookup** queries the configured name server for DNS information.

CCNA Discovery 2, Chapter 2

2.2.3: With the OSI reference model as a guide, you can define, isolate, and solve most network-related issues. As mentioned previously, you can approach an issue starting with the layer most likely to be the problem. If you are unfamiliar with the issue and its symptoms, the following bottom-up approach identifies key points to consider in each layer:

- **Physical layer (1):** Check power, connectivity, cables, LEDs, and environmental issues such as temperature and humidity.
- **Data link layer (2):** Check switch and NIC configurations and operation. Substituting a NIC or switch at this layer often can isolate the issue.
- **Network layer (3):** Check IP configurations on devices, and use commands such as **ping**, **ipconfig**, and **tracert** to test connectivity.
- **Transport layer (4):** If **ping** works, but an application still is not functioning, the issue may be a firewall and filtered TCP or UDP ports.
- **Layers 5 through 7:** Check the settings in your applications for encryption, authentication, or additional configuration requirements. You can also use Telnet to test Layer 7 functionality and network utilities such as a packet sniffer to analyze network traffic.

Differentiate Between LAN/WAN Operation and Features

Although LANs and WANs function together to create the Internet, they have different protocols and purposes. The better you understand the features of LANs and WANs, the better you will be at network design, configuration, and troubleshooting. Chapters 3 and 4 of *CCNA Discovery 1* and Chapter 5 of *CCNA Discovery 2* identify the main features of WANs and LANs.

CCNA Discovery 1, Chapter 3

3.1.6: As mentioned on Day 28, a network can be viewed from a physical and logical topology. A physical topology represents the location of the hardware, and the logical topology represents how the devices use the network.

3.5.5: A local-area network (LAN) can be one network in a single physical location or multiple networks under one administrative control. LANs today often represent the logical grouping of hosts for a single organization. Network administrators typically refer to the network they maintain in their building (or buildings) as a LAN or private intranet. LANs also support high data transfer rates over Ethernet or wireless protocols in a smaller geographic area. A wide-area network (WAN) provides relatively lower data transfer rates over a larger geographic area.

CCNA Discovery 1, Chapter 4

4.1.5: When an ISP provides services to a single user or an organization, it typically provides WAN connectivity. These connections to the ISP's network over a large geographic area can be symmetric or asymmetric. An asymmetric connection typically has a faster download speed than upload speed and works well for an Internet user who does not provide outgoing services over the connection. Symmetric connections provide the same upload and download speed; these connections are most often used by organizations or users who host servers and provide services to others.

CCNA Discovery 2, Chapter 5

5.5.3: Telecommunications service providers (TSP) typically maintain a network over large geographic areas. A TSP can provide the following WAN connections to individuals and organizations:

- A point-to-point (PPP) connection provides a specific dedicated path through the TSP network to connect two LANs over a large geographic area.
- A circuit-switched WAN connection allows the client to create and close connections over the TSP network; this connection operates like a phone call. Integrated services digital network (ISDN) is an example of a circuit-switched connection.

- A packet-switched WAN connection allows multiple clients to share a single connection. Unlike a circuit-switched network, in which the client temporarily uses the entire connection, a client on a packet-switched network uses a virtual circuit (managed by software) over a shared connection. Frame Relay is an example of a packet-switched connection.

Summary

A layered model helps you develop a structured plan to repair any network issue, whether it is a bottom-up, top-down, or divide-and-conquer approach. Your troubleshooting success also hinges on your knowledge of the protocols, connections, and configurations of LANs and WANs alike. Day 26 focuses on the common physical connections and ports you encounter on a network. You can further review the topics from today on pages 5–36 for the OSI model and pages 255–292 for WAN features in *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Part II

Days 26–21: Implement a small switched network

Day 26 covers network physical media

Day 25 covers media access control

Day 24 covers switch operation

Day 23 covers switch configuration

Day 22 covers switch security

Day 21 covers switch troubleshooting

Day 26

Select the Appropriate Media, Cables, Ports, and Connectors to Connect Switches to Other Network Devices and Hosts

Your choice to transmit data over fiber, copper, or radio waves can affect the speed, cost, and security of your network. In addition, any network upgrades will depend on the cables and port types you select for your network devices. Chapters 3 and 4 of *CCNA Discovery 1* and Chapter 3 of *CCNA Discovery 2* explain the common physical layer components for a network.

CCNA Discovery 1, Chapter 3

3.6.1–3.6.4: To plan an Ethernet network, you first determine how the network will be used. Gather information about the number of hosts, necessary applications, security needs, reliability requirements, and any wireless requirements.

As soon as you know why you are building the network, you need to plan the physical and logical topology. Consider the following points for each topology:

- For the physical topology, plan the proper environment (heat and temperature), availability of power, and device locations, cable connection distances and types, and device hardware configurations.
- For the logical topology, plan the size of each broadcast and collision domain, the IP addressing and naming schemes, sharing configuration, and permissions.

When your plan is complete, you can build a prototype using software such as Packet Tracer. If you choose to connect your network to a WAN, you can use an integrated services router (ISR) in your wiring closet. An ISR is capable of wireless connectivity and also has Ethernet ports for WAN connectivity and multiple Ethernet switching ports for LAN connectivity.

CCNA Discovery 1, Chapter 4

4.4.1–4.4.4: Table 26-1 identifies and defines common network cables.

Table 26-1 Common Network Cables

Cable Type	Description	Types
Twisted pair	Consists of multiple pairs of twisted wire that carry electrical signals. Inexpensive and easy to install, but susceptible to crosstalk and outside electrical interference. The twists in the wire pairs reduce crosstalk. Used for most LAN installations.	Category 5 unshielded twisted pair (UTP), Category 3 UTP, Category 6 UTP, and Category 7 screened twisted pair (ScTP). Terminated with an RJ-45 connector.
Coaxial	Carries electrical signals over a copper wire. Shielded and capable of longer lengths than UTP, but more expensive and difficult to install. Used for cable network offerings.	Coaxial cable terminated with a BNC type or F series connector.
Fiber-optic	Two fiber-optic cables to send and receive data with pulses of light. Consists of a coating, cladding, and glass core. Multimode is less expensive than single-mode fiber. Single-mode fiber is used for long distances and as backbone connections inside the building or between buildings.	Multimode runs a shorter distance with multiple rays of light from LEDs. 2000-meter limit. Single-mode provides a single path for an LED laser and can run a longer distance (3000 meters).

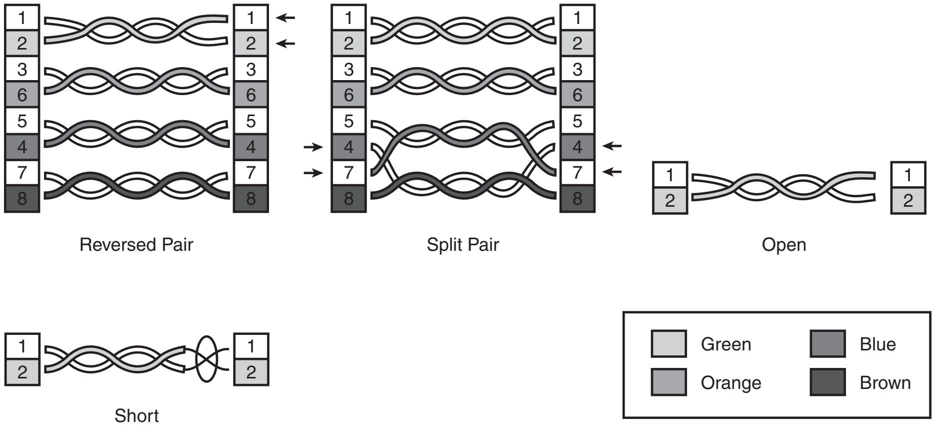
4.5.1: When you install the cabling for your network, it is important to follow cabling standards; these standards provide specifications for the installation and testing of cables. In addition, standards specify types of cables to use in specific environments, conductor materials, pinouts, wire sizes, shielding, cable lengths, connector types, and performance limits.

4.5.2: The following points define the standards for UTP cables:

- TIA/EIA defines the T568A and T568B wiring schemes for network cables. Be sure to use the same scheme for an entire installation project.
- A straight-through cable is wired with the same scheme on both ends, whereas a crossover cable is wired with T568A on one end and T568B on the other.
- You use a straight-through cable to connect unlike devices, such as a switch to a router. You use a crossover cable to connect like devices, such as PC to PC.
- Some devices can sense the pins available and adjust the port to work with either a crossover or straight-through cable.
- UTP cables typically are terminated with an RJ-45 jack that plugs into an RJ-45 connector.
- When you design your network, all your cables typically terminate in a patch panel, and you use patch cables to connect network devices.
- You use a punchdown tool to set the wires from a UTP cable properly in a patch panel. RJ-45 jacks typically come with a tiny punch tool or a cap that punches down the wires.
- You can test cables with a cable tester, cable certifier, or multimeter.

4.5.5: Figure 26-1 shows common wiring issues you may encounter with incorrectly terminated UTP cable.

Figure 26-1 Common UTP Wiring Issues



Crosstalk, mentioned previously, occurs when electrical signals leak between wire pairs. Near-end crosstalk (NEXT) occurs near the transmitting end of the cable, and far-end crosstalk (FEXT) occurs near the receiving end of the cable. FEXT and NEXT can result from overzealous untwisting of wire pairs when terminating a UTP cable.

Attenuation, or insertion loss, occurs as a signal travels over a cable. The signal encounters resistance and becomes weaker as it is transmitted through the cable.

4.5.6: Consider the following tips when terminating and installing cable:

- Install cables as far as possible from fluorescent lighting and high-voltage cables to avoid electromagnetic interference (EMI). Place cable runs that must be close to EMI in conduit.
- Adhere to cable length restrictions, install high-quality cable, test all installations, and label and record cable installations in your network documentation.

CCNA Discovery 2, Chapter 3

3.2.3: Backbone cabling between wiring closets is called *vertical cabling*. *Horizontal cabling* refers to the cables used to connect hosts and devices in the work area to the wiring closet. Consider the following points about each type of cable when you design your network's physical topology:

- **Shielded twisted pair (STP)** has foil shielding to protect from outside EMI and can be run for only 100 meters. STP can be Category 5, 5e, or 6 cable.
- **Unshielded twisted pair (UTP)** has no shielding and is also limited to 100 meters; however, UTP is inexpensive.

- **Coaxial** provides a shielded solid copper core for transmission and is not as limited by distance as UTP or STP.
- **Fiber-optic** cable is not affected by EMI, can run up to 3000 meters, and is capable of high-speed data transfer.

The following networking cables serve different purposes:

- **A crossover cable** connects similar devices: hub to hub, switch to switch, PC to PC.
- **A straight-through cable** connects devices that are not similar: hub to PC, switch to PC, switch to router.
- **A console cable** connects to the console port on a router or switch to configure the device.
- **A serial cable** is often used to connect a router to an Internet connection.

3.2.4: When designing a floor plan for your network, the following terms help define locations and cabling:

- The **Main Distribution Facility (MDF)** is the location of the main wiring closet, where you would place high-speed networking equipment and servers and possibly connect to other buildings, networks, or the Internet.
- The **Intermediate Distribution Facility (IDF)** is the location of a wiring closet where you would place networking equipment and servers for a specific area in your building and connect to the MDF.
- **Horizontal cables** run from the wall plate in the work area to the IDF.
- **Vertical cables** connect the IDF to the MDF as part of the network backbone that handles the most network traffic.

3.3.3: Choose Layer 2 devices for your network that allow the most efficient upgrades. Port speed, expandability, and cost are key factors in device selection. Consider modular devices that allow you to increase ports or change port type when you upgrade the network. A single switch with many ports may require cost-prohibitive cabling, whereas multiple switches could remove the risk of a single point of failure and require less cable. In addition, make sure that the cable infrastructure will support future upgrades in switches and routers.

Summary

Although UTP is the most common choice for LAN cabling, fiber and wireless connectivity can improve network performance and availability in certain areas. As soon as you have determined the location of your MDF and IDFs, you should be able to select the proper vertical and horizontal cabling to best serve the devices you will install in your network. You can further review network cable types on pages 71–84 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 25

Explain the Technology and Media Access Control Method for Ethernet Technologies

Ethernet media access control (MAC) defines how a transmission is prepared for the physical media. In addition, MAC defines when a device can transmit over the wire. A network device also uses the Ethernet protocol to decipher transmissions it receives. Chapter 3 of *CCNA Discovery 1* introduces the media access control method for Ethernet technologies.

CCNA Discovery 1, Chapter 3

3.2.1–3.2.8: Communication requires a source or sender, destination, and channel or pathway. As soon as you have a source, destination, and path, the next step is to develop a protocol for communication. The protocol defines the format, size, timing, encapsulation, encoding, and pattern for a message. In network communication the message is encoded into bits represented by electrical pulses and sound. A computer transmission is formatted as a frame. Figure 25-1 identifies the general fields of a frame.

Figure 25-1 Generic Frame

Destination	Source	Start Flag	Recipient	Sender	Data	End of Frame
Frame Addressing		Encapsulated Message				

If a data message is large, the communication protocol breaks it into multiple frames. Protocols also define when a device can communicate. If two devices communicate at the same time, a collision occurs, and they need to back off and start again. In addition, timing also determines how slowly or quickly a device can communicate. Last, a device can communicate with one other device through a unicast, with multiple devices through a multicast, or with all devices on a network through a broadcast.

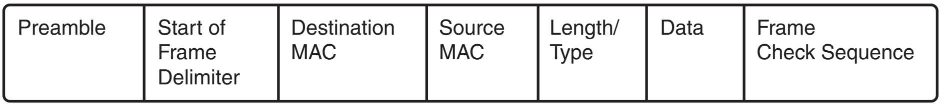
3.3.3: As mentioned on Day 28, hosts on Ethernet networks identify themselves with a media access control (MAC) address. All hosts on the network that receive the frame compare their MAC address to the destination address and respond if a match occurs.

3.3.4: The following points describe Ethernet protocol standards:

- An Ethernet frame is an OSI Layer 2 protocol data unit (PDU).
- An Ethernet frame maximum size is 1518 bytes, and minimum size is 64 bytes. Hosts do not process frames that are larger than 1518 bytes or smaller than 64 bytes.
- Ethernet standards also define how the bits of a frame are encoded on a channel: electrical signals over copper or light over fiber.

Figure 25-2 shows the field names for an Ethernet frame.

Figure 25-2 Fields of an IEEE 802.3 Ethernet Frame



- The **preamble** (7 bytes) of an Ethernet frame is used for sequencing and timing.
- The **start of frame delimiter** (1 byte) marks the end of the preamble and the beginning of the frame.
- The **source and destination MAC addresses** (6 bytes each) identify the sender and receiver.
- The **length field** (2 bytes) indicates how many bytes are left in the frame, and the **type field** (2 bytes) indicates the protocol that will receive the data.
- The **frame check sequence** (FCS) (4 bytes) is used to detect transmission errors with a cyclical redundancy check (CRC).

3.4.2: All devices connected on a hub are in the same collision domain. When Ethernet devices in the same collision domain attempt to communicate at the same time, a collision occurs. Each device detects the collision and waits a random amount of time before attempting to retransmit. Hosts on an Ethernet network use this process to ensure that only one host transmits at a time on a single collision domain. This process is often called carrier sense multiple access collision detect (CSMA/CD).

3.4.3–3.4.7: As covered on Day 28, switches build a MAC address table by reading the source address portion of a frame. As soon as a switch knows which port is connected to a device, the switch can create a temporary circuit between source and destination. Each port becomes its own collision domain, because the switch can forward multiple simultaneous transmissions on different circuits. A switch still floods broadcast frames and any frames with an unknown destination MAC address. Remember also from Day 28 that hosts with only an IP address use an ARP request to find the destination MAC and create a socket from the IP/MAC pair to identify the device.

Explain Network Segmentation and Basic Traffic Management Concepts

Collision and broadcast domains often define network boundaries. Just as the walls of meeting rooms keep conversations contained, devices that separate collision and broadcast domains keep device conversations over the network local. Chapter 3 of *CCNA Discovery 1* identifies the devices responsible for managing the traffic created in collision and broadcast domains.

CCNA Discovery 1, Chapter 3

3.4.4: Hosts on a single local network connected to a hub create a single collision domain. A switch increases the number of collision domains because it filters and forwards frames based on the source and destination MAC. However, switches still forward all frames with FFFF.FFFF.FFFF as the destination MAC address because it is a broadcast frame. When bandwidth needs or host numbers increase, broadcast traffic begins to slow a network. Routers do not forward broadcast frames; routers divide broadcast domains.

Summary

The Ethernet protocol provides a standard way for network devices to efficiently use the lines of communication in a network. A device can use frames and MAC addressing to communicate with one device on a LAN or all devices. Routers and switches ensure that local communication remains local while forwarding transmissions destined for other areas. You can further review the topics from today on pages 71–84 and 89–112 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 24

Explain the Operation of Cisco Switches and Basic Switching Concepts

You covered the basics of switches on Days 25 and 28. Switches are the central device in most modern local-area networks (LAN). This section describes the function of a switch as described in Chapter 3 of *CCNA Discovery 1* and Chapters 3 and 5 of *CCNA Discovery 2*.

CCNA Discovery 1, Chapter 3

3.4.3 and 3.4.4: The following key points, as highlighted on Day 28, are characteristics of a switch:

- An Ethernet device with multiple ports that de-encapsulates each frame to read the source and destination MAC addresses.
- A switch maintains a MAC table that tracks which hosts are attached to each port. The switch reads the source MAC address from an incoming frame and adds the address to the table as located at the incoming port.
- A switch uses the MAC address table to forward frames based on the destination MAC address.
- When two hosts on a switch communicate, the switch creates a temporary circuit between the devices and forwards only the frames between those ports. Not all hosts connected to a switch share bandwidth, because the switch creates these temporary circuits between communicating hosts.
- Multiple simultaneous conversations can occur without collisions because of the switch's capability to read the MAC address and create circuits, so each port is its own collision domain on a switch.
- If the switch does not yet know the port for a frame's destination MAC address, it floods the frame out all other ports.
- Switches do not forward frames with errors or frames with the same source and destination.
- If you connect a hub to a switch port, the switch associates all MAC addresses of devices connected to the hub with that port. Any traffic between devices connected to the hub is repeated to the switch, but the switch recognizes that the frames have the same switch port as the source and destination and does not forward the frame. Collisions still occur on the hub and are repeated, but the switch does not forward the damaged frames.
- Switches forward a frame with the MAC address FFFF.FFFF.FFFF because it is a broadcast address identified by the sending host as destined for all other hosts on the network.

CCNA Discovery 2, Chapter 3

3.3.3: A modular switch can have fixed ports as well as expansion slots. You could use an expansion slot to later upgrade to a higher-speed set of ports or fiber-optic modules. Managed switches allow the administrator to restrict access to ports, turn off a port, and monitor traffic for performance and security.

CCNA Discovery 2, Chapter 5

5.4.1: A switch deals with MAC addresses and frames at OSI Layer 2. A standard switch does not route traffic at Layer 3 of the OSI model and cannot route traffic between two different LANs.

A typical switch for medium-sized businesses and branch offices is a 2960 series switch. These switches have a fixed hardware configuration, can provide up to Gigabit Ethernet connectivity for hosts, and allow software configuration through Cisco IOS software or the GUI-based Cisco Network Assistant. Remember the following key points about switch ports:

- A switch port can operate in full-duplex mode, allowing it to send and receive data simultaneously.
- A switch port can also operate in half-duplex mode, allowing the port to alternatively send and receive data, but not send and receive simultaneously.
- When a device is connected to a switch, the switch attempts to autonegotiate the speed and either full- or half-duplex transmission. If the other device does not support autonegotiation, the switch defaults to the speed of the other device and half duplex.
- An administrator can turn off autonegotiation and manually set the switch to full or half duplex.
- If a connected device is incapable of autonegotiation, you can set the switch to the device's matching duplex, and the switch adjusts for the connection speed.

Summary

When you select a switch for your network, keep in mind the ports you will need in the future and the bandwidth your network will require. Days 23, 22, and 21 will take you past the concepts of switch selection to switch configuration and troubleshooting. You can further review the topics from today on pages 89–112 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 23

Perform, Save, and Verify Initial Switch Configuration Tasks, Including Remote-Access Management

You can plug a switch into your network straight out of the box, and it will forward frames fabulously. However, talented and good-looking administrators always configure additional features on a switch to provide security and remote-access management. Chapter 5 of *CCNA Discovery 2* explains the methods available and steps to configure a switch for secure remote management.

CCNA Discovery 2, Chapter 5

5.3.1: The Cisco IOS command-line interface (CLI) provides the following configuration modes:

- **User access or user EXEC:** When you power up a switch, you receive user access by default. In this mode you can only execute commands that show basic information about the operation of the device or test connectivity. The CLI prompt for this mode looks like this:

  ```
  router>
  ```

- **Privileged EXEC:** If you enter **enable** at the prompt for user access, you enter privileged EXEC mode. This mode allows you to adjust the operation of a switch and view additional information about a switch, including configuration files. The CLI prompt for this mode looks like this:

  ```
  router#
  ```

- **Global configuration:** If you enter **configure terminal** at the privileged EXEC prompt, you enter global configuration mode. This mode allows you to configure the device and enter submodes for specific configurations. The CLI prompt for this mode looks like this:

  ```
  router(config)#
  ```

- **Submodes of configuration mode:** As soon as you are in configuration mode, commands such as **interface** and **router rip** allow you to enter specific submodes. The following are examples of the interface configuration and routing protocol configuration submode prompts:

  ```
  router(config-if)#
  ```

  ```
  router(config-router)#
  ```

5.4.2: To configure a switch, you need to connect the switch to power. When the switch first powers up, it runs through a power-on self-test (POST), and the SYST LED should blink green. If the SYST LED turns amber, the POST has failed.

5.4.3: Initially you have to connect to the switch through the console port with a PC running terminal emulation software. You can then configure a management IP address on the switch and configure the switch with web- or network-based configuration tools. The following methods allow you to configure a switch:

- **Cisco IOS software CLI:** You can access the CLI by directly connecting to the switch or by using Telnet after you have configured a management IP address. This option provides command-line access to Cisco IOS software and allows you to configure and monitor all aspects of the switch or a group of switches.
- **Cisco Network Assistant:** This is a graphical user interface (GUI) that you can download for free from Cisco.com. It helps you manage a single switch or group of switches. The software is intended for small and medium-sized businesses.
- **Cisco Device Manager:** This software is located on the switch and can be accessed with a web browser to manage a single switch. Web access to a switch is available only after you configure a management IP address.
- **CiscoView Management Software:** This is software purchased separately that can be run for a single switch or as a Simple Network Management Protocol (SNMP) product.
- **SNMP products:** Large companies use programs such as HP OpenView or SunNet Manager to manage large networks.

The switch will already have an initial configuration; you only need to add a management IP address and basic security information. By default, a switch has only one virtual local-area network—VLAN 1. You access the switch by IP address on VLAN 1 for management through Telnet or other IP-based management software. Example 23-1 demonstrates the commands necessary to perform the initial configuration on a switch, including an IP address and default gateway on VLAN 1.

Example 23-1 Initial Configuration on a Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname Switch22
Switch22(config)# line console 0
Switch22(config-line)# password cisco
Switch22(config-line)# login
Switch22(config-line)# line vty 0 4
Switch22(config-line)# password cisco
Switch22(config-line)# login
Switch22(config-line)# exit
Switch22(config)# enable password cisco
Switch22(config)# enable secret class
Switch22(config)# interface vlan 1
Switch22(config-if)# ip address 192.168.1.2 255.255.255.0
Switch22(config-if)# no shutdown
Switch22(config-if)# exit
Switch22(config)# ip default gateway 192.168.1.1
Switch22(config)# exit
Switch22# copy running-config startup-config
```

Verify Network Status and Switch Operation Using Basic Utilities (ping, traceroute, Telnet, SSH, ARP, ipconfig, show, and debug Commands)

As soon as the network is running and your switch is configured properly, you may need to troubleshoot connectivity from time to time. Chapter 9 of *CCNA Discovery 1* describes some of the utilities available on most hosts to verify network configurations and operation. Chapter 5 of *CCNA Discovery 2* discusses the commands available to verify your configuration on a switch.

CCNA Discovery 1, Chapter 9

9.2.3–9.2.5: The following commands allow you to troubleshoot your network connection:

- The **ipconfig** command allows you to view the IP configuration on a host that is running the Windows operating system. Use the command **ipconfig /all** to view the MAC address and DHCP and DNS information. To release the IP address obtained from a DHCP server, use the command **ipconfig /release** at the prompt. Then use the command **ipconfig /renew** to attempt to receive a new configuration from a DHCP server.

- The **ping** command allows you to test Layer 3 connectivity between devices. You can ping an IP address, or, to test a host's capability to resolve DNS, you can ping a domain name. Ping tests connectivity with an echo request and echo reply. You can enter **ping** at the command prompt without an IP address or domain for advanced options.

- The **traceroute** command on a router or switch allows you to test connectivity for each hop between two devices. Microsoft Windows uses the command **tracert** to test hops between devices.

- The **arp -a** command on a host shows all ARP entries for that host. You can enter **arp** at the prompt for additional options.

CCNA Discovery 2, Chapter 5

5.4.3: If you are unable to ping hosts on your switch, you can use the following **show** commands in privileged EXEC mode on a switch to view the configuration:

```
show running-config
show startup-config
show interface vlan 1
```

After you have configured an IP address and the vty password, you can test connectivity and remote access on a switch with **ping**, **telnet,** and **ssh**. In addition, you can check the Cisco IOS software version on a switch with the **show version** command.

Summary

You have completed the difficult part when your network is wired and all hosts are connected to the switch. The fun starts when you have the opportunity to secure, monitor, and maintain your network with the advanced features provided in today's advanced switches. To say a switch should only be connected and left alone is like saying an apple tree is only for shade. Pick the fruit: Configure those advanced features on your switch. You can further review the topics from today on pages 115–126 and 129–172 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 22

Implement and Verify Basic Security for a Switch (Port Security, Deactivate Ports)

On Day 23 we discussed password protection for switch management. Today we take that security a step further and prevent an unauthorized user from connecting to the switch in the first place. Chapter 5 of *CCNA Discovery 2* explains how to secure ports on your switch.

CCNA Discovery 2, Chapter 5

5.4.3: As soon as a switch is properly configured and connected in the wiring closet, an unauthorized user could connect to a wall jack and attempt to access the network. You can enable a feature called **port security** to limit the number of MAC addresses that a switch can learn for each port. If you set the MAC address to port ratio to 1, the switch recognizes only the first MAC address it learns as the secure address. Port security is similar to MAC address filtering on a Linksys device. You can manually configure a MAC address for each port, or you can allow the switch to dynamically learn the MAC address. You can view and clear the MAC address table on a switch with the following commands in privileged EXEC mode:

```
show mac-address-table
clear mac-address-table
```

You can use the following command to assign a static MAC address to an interface:

```
mac-address-table static {host-mac-address} interface {interface} vlan {vlan}
```

For example:

```
Switch(config)# mac-address-table static 00F1.1111.2323 interface FastEthernet
  0/3 vlan 1
```

To view all options for the **mac-address-table** command, enter the command and add a question mark (**?**) after the command. Use the command **no** in front of the **mac-address-table** command to remove the static MAC address configuration. If you enable sticky learning on a switch, the first MAC address it learns becomes the secure address. The following commands set up port security and enable sticky learning:

```
switchport mode access
switchport port-security
switchport port-security mac-address sticky
```

For example:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address sticky
```

Remember that you can enter **switchport port security ?** to view all options for the command. Also, the following commands allow you to verify your configuration:

```
show port-security
show running-config
show interfaces
show vlan
```

If an unauthorized device attempts to connect to the port and the switch shuts down the port, you can use the **no shutdown** command to reactivate the port:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/3
Switch(config-if)# no shutdown
```

You could also manually shut down a port with just the **shutdown** command used in the same manner as the preceding example. In addition, you can control the speed and duplex of a port with the following commands:

```
speed {speed-in-megabits-per-second}
duplex {half ¦ full}
```

For example:

```
Switch(config)# interface fastethernet 0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

You can save your configuration with the **copy running-config startup-config** command. However, if your configuration is incorrect and you want to start over, you can delete VLAN database information and erase the startup configuration with the following two commands in privileged EXEC mode:

```
delete flash:vlan.dat
erase startup-config
```

Summary

As your network grows and multiple users move around and add devices to or remove devices from the jacks in the wall, port security allows you to manage the devices that come and go on your network. Switches allow you to control access using the MAC address of each device as an identifier and stop intruders at Layer 2. The information covered on Day 23 and today should give you the tools to better manage and secure a switched network. You can further review the topics from today on pages 129–172 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 21

Identify, Prescribe, and Resolve Common Switched Network Issues, Autonegotiation, and Switch Hardware Failures

When the network stops and all the hosts stop talking, it is time to take a look at your switch. The troubleshooting process should start at Layer 1 with switch hardware issues and continue to Layer 2 with possible switch software or configuration issues. Chapter 9 of *CCNA Discovery 1* and Chapters 2 and 5 of *CCNA Discovery 2* explore troubleshooting options for you and your switch.

CCNA Discovery 1, Chapter 9

9.2.1: You will likely identify some serious switch hardware problems with your senses. Hot, loud, lightless switches can indicate problems with your switch hardware. Check for a malfunctioning fan, possible overheating, and faulty power or network connections.

9.3.1–9.3.3: The following test can help you isolate issues on a switched network:

- Look at LED indicators on your networking devices. LEDs can show network or processing activity, power, and the status of a device. An inactive LED can indicate power or hardware failure as well as an improper configuration for a port or connection.
- To check connectivity issues, you should ping your default gateway to ensure connectivity between your host and the router. You can then ping other hosts and a domain on the Internet to check connections among your router and other devices.
- Check the types of cables in use on your network. Remember the proper uses for straight-through, crossover, and console cables. In addition, check that the cables are not beyond the maximum length, are properly terminated, and are connected to the correct ports on your device.

CCNA Discovery 2, Chapter 2

2.2.3: Layer 2 troubleshooting involves the network interface cards (NIC) in hosts on the network and your network switches. A quick way to isolate the issue is to replace a NIC or switch that appears faulty and test connectivity on the network. Although replacing a NIC is cost-effective, you might want to check the configuration and software on a switch before replacing the device.

CCNA Discovery 2, Chapter 5

5.4.4: The commands listed in Table 21-1 allow you to verify the function and configuration of a switch.

Table 21-1 Switch Troubleshooting Commands

Command	Definition
show running-config	Displays the running configuration stored in RAM on the switch.
show startup-config	Displays the startup configuration stored in NVRAM on the switch.
show version	Displays the Cisco IOS software version and image name as well as information about the memory and processor on a switch.
show interfaces	Displays information about the interfaces on a switch, including security and addressing.
show mac-address-table	Displays MAC table entries on a switch.
show port-security	Displays port security settings on a switch.
show cdp	Displays whether Cisco Discovery Protocol (CDP) is running on your switch. Does not display information about connected neighbors.
show cdp neighbors	Uses Layer 2 CDP communication to discover and display information about directly connected Cisco devices and their platforms.
show cdp neighbors detail	Displays detailed information about connected Cisco devices, including the Layer 3 IP address.

As outlined in Table 21-1, CDP can verify Layer 2 connectivity even when a Layer 3 IP address is not properly configured. You can also use CDP to learn about the hardware and software configuration of connected devices with CDP enabled. You can disable CDP globally on your switch with the following command from global configuration mode:

```
no cdp run
```

You can disable CDP on a specific interface with the following command in interface configuration mode:

```
no cdp enable
```

Summary

As soon as you have checked for hardware issues with a switch, it is important that you thoroughly check your switch configuration with the **show** commands discussed today. Sometimes other administrators control neighboring switches. CDP allows you to peek at some of their configuration information and see if the issue is their problem or yours. When everything looks good on your end, do not forget the powers of CDP. You can further review the topics from today on pages 129–172 and 315–342 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Part III

Days 20–13: Implement an IP addressing scheme and IP services to meet network requirements for a small branch office

Day 20 covers IP addressing

Day 19 covers assigning addresses

Day 18 covers NAT

Day 17 covers DNS operation

Day 16 covers private networks and NAT

Day 15 covers DHCP operation

Day 14 covers static and dynamic addressing

Day 13 covers IP address troubleshooting

Day 20

Describe the Need for and Role of Addressing in a Network

Just as with the postal system, no address means no delivery on a network. As a network administrator, you have the unique opportunity to give unique numeric names to each of your beloved devices. These names, or IP addresses, become known throughout your network and represent the services and devices cooperating to provide information to your users. Network addressing is an exciting activity. Chapters 2 and 5 of *CCNA Discovery 1* introduce the main concepts of network addressing.

CCNA Discovery 1, Chapter 2

2.2.5: Each host on a network requires a unique name and logical address to communicate over a network. A consistent format in your addressing scheme makes it easier to locate a device and troubleshoot network issues.

CCNA Discovery 1, Chapter 5

5.1.1: The IP address typically is assigned to the network interface card (NIC). In addition, routers need an IP address for each interface. Layer 3 packets include a destination and source IP address used by routers to determine the path over the network.

5.1.2: An IP version 4 (IPv4) address is made up of 32 binary bits. These bits are divided into four octets (8 bits) and are represented in decimal format. Table 20-1 shows one octet of an IP address and the math used to convert the octet to decimal. The value of each bit in an octet is determined by the powers of 2 from right to left. If there is a 1 in the bit, the value is added to the decimal equivalent. If the bit is a 0, the value is not added to the decimal equivalent.

Table 20-1 Octet Converted to Decimal

Bits and Powers of 2								Decimal Equivalent
1	1	1	1	1	1	1	1	128+64+32+16+8+4+2+1 = 255
128	64	32	16	8	4	2	1	
1	0	1	0	1	0	0	0	
128	64	32	16	8	4	2	1	128+0+32+0+8+0+0+0 = 168

The minimum decimal equivalent for an octet is 0, and the maximum is 255. Table 20-2 shows an IP address in dotted-decimal format and its binary equivalent.

Table 20-2 Decimal and Binary Representation of an IPv4 Address

Decimal	Binary
192.168.1.12	11000000.10101000.00000001.00001100

5.1.3: An IP address contains a network portion and host portion. The first part is the network portion, and the second part is the host portion. You determine the network portion with the subnet mask. A subnet mask is a 32-bit address that uses binary 1s to identify the network portion. Simply put, the bits in a subnet mask with a value of 1 represent the network portion of the IP address. Table 20-3 shows an IP address and how the subnet mask is used to determine the network address. This is also called ANDing because of how the mask and address are combined to calculate the network address.

Table 20-3 Using the Subnet Mask to Determine a Network Address (ANDing)

Decimal IP Address and Subnet Mask	IP address 192.168.2.38 Mask 255.255.255.0
Binary IP Address	11000000.10101000.00000010.00100110
Binary Subnet Mask	11111111.11111111.11111111.00000000
Binary and Decimal Result	Result 11000000.10101000.00000010.00000000 Network address 192.168.2.0

Routers use the subnet mask to determine the network address of a destination IP address and where to forward the packet. All networks need a network address and an address for broadcasts. The network address has all 0s in the host portion, and the broadcast address has all 1s in the host portion. Remember to subtract these two addresses from the available host addresses when designing a network. For example, the network in Table 20-3 has the entire last octet for the host addresses minus the network address (192.168.2.0) and the broadcast address (192.168.2.255), so 254 host addresses are available from the 256 possible combinations.

Create and Apply an Addressing Scheme to a Network

The addresses and subnet masks you use in your network define the logical organization of the devices on your network. Courteous, intelligent, stylish network administrators always follow the guidelines necessary to properly identify hosts and subnetworks within a network. Chapter 5 of *CCNA Discovery 1* and Chapter 4 of *CCNA Discovery 2* provide the guidelines to follow when creating and applying an addressing scheme to your network.

CCNA Discovery 1, Chapter 5

5.2.1 and 5.2.2: You can identify networks quickly as Class A, B, or C networks using Table 20-4. These default network classes have a default subnet mask and a specific network-to-host ratio. You would use a Class A network for a maximum number of hosts and a Class C network for a smaller network that needs only a few hosts. Class D and E networks are not for commercial use.

Table 20-4 Class A, B, C, D, and E Networks

Class	Binary Start	First Octet Range	Subnet Mask and Network (N) and Host (H) Octets	Number of Hosts	Bits in the Network Address
Class A	0	1–126	255.0.0.0 N.H.H.H	16,777,214	8
Class B	10	128–191	255.255.0.0N.N.H.H	65,534	16
Class C	110	192–223	255.255.255.0N.N.N.H	254	24
Class D	1110	224–239	H.H.H.H	Multicast	—
Class E	1111	240–255	RESEARCH	RESEARCH	RESEARCH

Request For Comments (RFC) 1918 identifies the networks reserved for internal or private use. A company or office can use the private networks identified in Table 20-5. However, to connect the private network to the Internet, you would need to attach a router with a public IP address and network address translation (NAT) capabilities. A router can forward only public IP addresses on the Internet. In addition, Class A network 127.0.0.0 is used for internal diagnostics on a device. If you ping 127.0.0.1 on your device, you are testing the internal functionality of your host's NIC and software. The diagnostic address 127.0.0.1 is called the loopback address.

Table 20-5 RFC 1918 Private Networks and the Loopback

Class	Address Range
Class A	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255
Loopback	127.0.0.0 to 127.255.255.255 (ordinarily 127.0.0.1 is used as the loopback address)

5.2.3: An IP address can also be categorized as a unicast, broadcast, or multicast address. The following key points define each category:

- A **unicast** IP address is the most common category of addresses used on a network. Devices use unicast addresses to communicate with one other device; a unicast address facilitates one-to-one communication over a network.
- **Broadcast** IP addresses contain all 1s in the host portion of the address. Devices use broadcast addresses to communicate with all hosts on a network. Protocols that request information from all hosts on a network, such as Address Resolution Protocol (ARP) and Dynamic Host

Configuration Protocol (DHCP), use broadcast addresses. A broadcast IP address has a corresponding broadcast MAC address of FF-FF-FF-FF-FF-FF on an Ethernet network. All-1s broadcasts are not forwarded by routers to other networks. Directed broadcasts are forwarded to remote networks until they reach an attached router, which then changes the destination address to an all-1s address before sending the packets out on the locally attached wire.

- If you assign addresses from the Class D range to hosts on a network, these hosts become part of a **multicast** group. These devices can then send multicasts to the hosts in the group. You might use multicasts for videoconferencing or remote gaming. The corresponding MAC address for multicasts begins with 01-00-5E.

CCNA Discovery 2, Chapter 4

4.1.1–4.1.4: When you create a logical design for a network, you will likely use a 32-bit hierarchical IP addressing scheme. The size of your network and the need for host addresses will dictate the class of network you choose and the number of bits necessary for the network and host portions of your IP addresses. As soon as you have determined the potential need for hosts, you can identify the network portion of the addresses with a subnet mask. If you started with a Class A address, you can further divide the Class A network into multiple Class B networks by using a Class B subnet mask. Table 20-6 demonstrates how you might divide a Class A network into four smaller networks.

Table 20-6 Dividing a Class A Network

Class A Network and Default Mask	Four Smaller Networks Created from a Class A Network
10.0.0.0 255.0.0.0	10.1.0.0 255.255.0.0
	10.2.0.0 255.255.0.0
	10.3.0.0 255.255.0.0
	10.4.1.0 255.255.255.0

When you divide a network beyond its default class, you use bits from the host portion as network bits. The router looks at the new mask and determines the network address regardless of the default class; this is called Classless Interdomain Routing (CIDR). Notice that the last of the smaller networks in Table 20-6 has a different size subnet mask. When dividing networks, you can also use variable-length subnet masks (VLSM). In Table 20-6 the Class A subnet mask uses 8 bits, and the new mask for the smaller network uses 16 bits. Another way to represent the Class A network from Table 20-6 is 10.0.0.0/8, and the first smaller network could be represented as 10.1.0.0/16. The slash followed by the bit number is often called *slash notation*.

You could also use CIDR with VLSM to divide a Class C network into smaller networks by borrowing bits from the host portion of the address to use in the network portion. A default Class C network has a 24-bit subnet mask represented as 255.255.255.0. The entire last octet provides 254 host addresses if you subtract the network and broadcast addresses. If you borrow bits from the host portion, the subnet mask reflects the bits that you have borrowed, and you will have more networks, but fewer hosts for each network. Table 20-7 provides the resulting networks and hosts if you increase the number of bits for the network portion of the address. Remember to subtract 2 from the available hosts in a subnet; each subnet needs a network and broadcast address.

Table 20-7 Borrowed Bits to Divide a Default Class C Network

Slash Format	/25	/26	/27	/28	/29	/30	/31	/32
Last Octet in the Mask (in Decimal)	128	192	224	240	248	252	254	255
Bits Borrowed	1	2	3	4	5	6	7	8
Total Subnets	2	4	8	16	32	64	—	—
Total Hosts	128	64	32	16	8	4	—	—
Usable Hosts	126	62	30	14	6	2	—	—

You can determine all the information in Table 20-7 by using the binary representation and the powers of 2. For example, the /26 network means that there are 26 bits total for the network portion (remember that a default Class C network uses 24 bits). You have borrowed 2 bits from the last octet and changed them from host bits (0) to network bits (1), so the last octet of the mask is the decimal representation of 11000000, or 192. To find the number of subnetworks available, you can insert the number of bits borrowed (n) into the formula 2^n. In this case, the result is four available subnetworks. If you look at the number of 0s in the mask 11000000, you can place those remaining bits in the formula 2^n–2. You will find that you have 62 hosts available per network.

To continue with the example of 2 bits borrowed, you can also determine the subnetworks and host ranges using the mask. In this case you can use host bits (0s) available in the last octet and apply the formula 2^n. This gives you an interval of 64. Using this interval, you can start with the zero subnet and then add 64 to identify your networks. Table 20-8 provides an example of the subnetworks and host ranges available for the default Class C network 192.168.1.0 with 2 bits borrowed. Remember that the subnetwork ID (all 0s in the host portion) and broadcast address (all 1s in the host portion) cannot be assigned to an interface.

Table 20-8 Subnetworks for 192.168.1.0 with 2 Bits Borrowed (255.255.255.192 Mask)

Subnetwork Number	Subnetwork ID	Host Range	Broadcast
0	192.168.1.0	.1–.62	192.168.1.63
1	192.168.1.64	.65–.126	192.168.1.127
2	192.168.1.128	.129–.190	192.168.1.191
3	192.168.1.192	.193–.254	192.168.1.255

4.1.5: A properly created subnetwork operates like any other network. You need a router to communicate between subnetworks, clients on a subnetwork need a default gateway, and each subnetwork is its own broadcast domain.

4.1.6: In 1998, RFC 2460 proposed IPv6. IPv6 increases address space, is easier to manage, and improves multicasting and security. The following key points generally define an IPv6 address:

- IPv6 addresses are 128-bit addresses represented as 32 hexadecimal digits.
- The 32 hex digits representing an IPv6 address are broken into eight groups of four digits separated by colons.
- IPv6 addresses have three parts. The **global prefix**, assigned to an organization, is the first three blocks. The **subnet identifier** is controlled by the network administrator. The **interface identifier** is also controlled by the network administrator.

Summary

First you decide how many networks you need. Then you determine the subnet mask that will allow enough hosts on each network. Finally, you list the host addresses available for each network. It is a good idea to map out your addressing scheme on a piece of paper before doling out addresses to hosts. A good addressing scheme allows for growth, efficiently uses available address space, and follows an organized format. Good addressing leads to efficient troubleshooting, better security, and more uptime for your precious, yet forever impatient, users. You can further review the topics from today on pages 193–216 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 19

Assign and Verify Valid IP Addresses to Hosts, Servers, and Networking Devices in a LAN

After you have developed a logical topology and proper addressing scheme, you must assign the addresses to devices on your network. Chapters 2 and 5 from *CCNA Discovery 1* as well as Chapter 5 from *CCNA Discovery 2* discuss the concepts and general steps to assign and verify IP addresses for devices in a LAN.

CCNA Discovery 1, Chapter 2

2.2.3 and 2.2.4: After you have physically connected a host to your network, you need to assign an IP address, default gateway, and subnet mask. You can manually enter the address information or configure the host to obtain address information dynamically. A host typically acquires address information dynamically from a Dynamic Host Configuration Protocol (DHCP) server. The operating system on some hosts allows you to enter a unique name for your computer.

CCNA Discovery 1, Chapter 5

5.3.1: Static address assignment on a host guarantees that it will always have the same IP address on the network. Hosts that provide services such as servers and printers usually receive static IP addresses. However, large networks typically add and remove hosts for various purposes, so DHCP provides a manageable way to maintain the addressing scheme.

To verify the IP configuration on a host running a recent Microsoft Windows operating system, you can open a command prompt and use the following command:

```
ipconfig /all
```

5.4.1 and 5.4.2: The default gateway for a host is typically the IP address of the connected interface on the router for the network. Each host on the network can then use the router as the gateway to other networks. Often the router acts as the DHCP server and provides addresses to hosts on the local network. On the other hand, the router connects to the Internet service provider (ISP) as a DHCP client to obtain an outside IP address. The following three methods are the most common ways for a user to connect to an ISP:

- **Direct connection to a modem:** A single host connects to the modem, which provides a direct connection between the host and the ISP. The host obtains an outside (Internet-routable) IP address from the ISP.

- **Connection to a modem, to a router, or to hosts:** The modem connects to a router, and the router obtains an outside IP address from the ISP. The router acts as the DHCP server and acts as the gateway for local hosts.

- **Gateway device:** A router with an integrated modem connects to the ISP and obtains an IP address. The router acts as the DHCP server and gateway for connected local hosts.

CCNA Discovery 2, Chapter 5

5.3.4 and 5.4.3: All graphical interfaces used to assign addresses vary, but the following general commands allow you to assign an IP address to an interface in the Cisco IOS software:

```
enable
configure terminal
interface interface
ip address ip-address subnet-mask
no shutdown
```

We covered an example of switch IP address configuration on Day 23, and we will cover an example of router interface configuration on Day 10. The following commands allow you to verify interface configuration:

```
show interfaces
show running-configuration
show startup-configuration
```

Summary

Today you read about the concepts of static and dynamic addressing. How you decide to address your network depends on the purpose of each device, the configuration tools available, and the goals of your users. You can further review the topics from today on pages 39–68 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Explain the Basic Uses and Operation of NAT in a Small Network Connecting to One ISP

Most home networks and many small business networks implement Network Address Translation (NAT) to preserve IP addresses and provide a basic level of security. Chapter 5 of *CCNA Discovery 1* and Chapters 4 and 5 of *CCNA Discovery 2* discuss the operation and uses of NAT in a small network.

CCNA Discovery 1, Chapter 5

5.2.2: As mentioned on Day 20, you can assign a private addressing scheme to an internal network; however, these addresses cannot be routed over the Internet. Table 18-1 displays the reserved addresses for private networks.

Table 18-1 RFC 1918 Private Networks

Class	Address Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

If you create a private network with one of these address ranges, your internal hosts can still connect to the Internet through a router configured for NAT. A router can receive a public Internet-routable address from the ISP and provide Internet connectivity for the hosts on the local private network. The router uses NAT to exchange private IP addresses for a public IP address or a pool of public IP addresses. This change (or translation) of the address allows an internal host to appear as though it has a public IP address for the purpose of Internet communication. In addition, NAT can provide security, because an outside computer on the Internet cannot discover the private IP address of a host on the internal network.

CCNA Discovery 2, Chapter 4

4.2.1: NAT was developed to preserve public IP addresses. A company with numerous hosts that communicate over the Internet only intermittently can save money and provide additional security by using NAT to share public IP addresses among privately addressed hosts. Table 18-2 explores the advantages and disadvantages of NAT.

Table 18-2 Advantages and Disadvantages of NAT

Advantages	Disadvantages
Reduces cost for additional public IP addresses	Incompatible with some complex network applications and types of remote access
Provides additional security and local control of Internet traffic	Can reduce performance for a connection
Allows for easier LAN expansion	Can frustrate legitimate remote access

4.2.2: The following terms define the various addresses and networks used in NAT:

- **Inside local network:** The privately addressed internal network connected to a router.
- **Inside local address:** A private internal IP address assigned to hosts attached to the inside local network.
- **Outside global network:** Any network outside the local network that would also not recognize the private addresses assigned to hosts in the local network.
- **Inside global address:** An IP address of a host attached to the local internal network as it appears to the outside network. The translated IP address.
- **Outside local address:** The destination address of the packet while on the inside local network. Typically the same as the outside global address.
- **Outside global address:** The actual destination address of the intended external host on the Internet.

4.2.3: Table 18-3 identifies the features of static and dynamic NAT. Both types of NAT can be configured at the same time.

Table 18-3 Features of Static and Dynamic NAT

Static NAT	Dynamic NAT
Translation for one private address to one public address	The router has a pool of public addresses to temporarily assign for internal hosts to communicate with an outside network
Allows internal hosts to provide services to remote devices on the Internet	When an internal host ends the communication with the outside network, the public address returns to the pool
Guarantees that no other internal host will use the reserved public address	—

4.2.4 and 4.2.5: If you intend to configure a router to translate one public IP address for many internal hosts, you can implement NAT overload, or port address translation (PAT). A router uses PAT to allow multiple internal hosts to communicate with just one public IP address. The router receives the request for communication from the internal host and uses source port numbers to identify the internal connection request. An outside computer could not reliably initiate a connection with an internal host, because the source port used by the router can change with each request, so internal hosts must initiate communication with outside networks. With more than 64,000 port numbers available, a router can translate with PAT for as many internal hosts as its processor and bandwidth can handle. Some applications include additional IP address information in encapsulated data, increasing the load on a router processor. Make sure you choose a router that can handle the external traffic expected on your network if you intend to use PAT.

CCNA Discovery 2, Chapter 5

5.3.8: One reason you may want to configure static NAT is to assign a public address to a server connected to your private network. To configure static NAT, you have to designate an inside interface—the interface connected to the private network. You also designate the interface connected to the outside world as the outside interface. As soon as you have properly configured IP addresses on your router interfaces, use the following commands to configure static NAT:

```
ip nat outside
ip nat inside
ip nat inside source static local-IP-address global-IP-address
```

For example:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip nat outside
Router(config-if)# interface fa 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source static 192.168.1.5 209.165.200.226
```

As mentioned previously, NAT with overload enables PAT. You use the **access-list** command to define the private address pool that you want to translate to a single IP address. An access list uses a wildcard mask instead of a subnet mask to identify the bits available for use as hosts in the pool. As soon as the IP addresses on your network and router are properly configured, you can configure NAT with overload using the following commands:

```
access-list access-list-number permit inside-network wildcard-mask
ip nat inside source list access-list-number interface interface overload
ip nat outside
ip nat inside
```

For example, the following commands first identify the pool of private addresses with an access list and then specify the inside and outside interfaces:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface serial 0 overload
Router(config)# interface serial 0
Router(config-if)# ip nat outside
Router(config-if)# interface fa 0/0
Router(config-if)# ip nat inside
```

The following commands allow you to verify NAT configuration and operation:

```
show running-config
show ip nat translation
debug ip icmp
ping
```

The **debug ip icmp** command outputs any Internet Control Message Protocol (ICMP) traffic processed by the router, including ping traffic. If you execute this command on the router and then ping an outside address from an internal host, the router outputs ICMP packet information to a terminal. When you are done troubleshooting, remember to turn off any debugging with the **undebug all** command.

Summary

NAT allows you to experience the freedom and increased address space of a private network, yet still enjoy Internet connectivity for all your hosts. In addition, you can provide basic protection for your internal hosts with a network design that includes NAT. NAT has quickly become standard for at least some portions of small networks connected to one ISP. You can further review the topics from today on pages 255–292 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 17

Describe and Verify DNS Operation

Although IP addresses do the job for computers, people like names with meaning to identify their websites and servers. The hierarchy of Domain Name System (DNS) provides a structured way to give people-friendly names to the devices that provide services on a network. Chapter 9 of *CCNA Discovery 1* and Chapter 7 of *CCNA Discovery 2* discuss DNS.

CCNA Discovery 1, Chapter 9

9.2.7: A network application such as a browser usually relies on a domain name to request Internet services. The host usually contacts a DNS server to match a network IP address to the domain or to resolve the domain. You can test a host's capability to access a DNS server with the nslookup utility. At the command prompt on a host, enter **nslookup** followed by a domain name to test DNS operation on your network.

CCNA Discovery 2, Chapter 7

7.3.1: As mentioned, a domain name such as cisco.com is easier to remember than an IP address. Each network host contains a HOSTS file that matches names to IP addresses. This HOSTS file is scanned first by the host to resolve a request for a domain. However, this HOSTS file contains a very limited list of names and IP addresses, so a DNS server performs the bulk of domain resolution on a network.

7.3.2: DNS operates using a hierarchical structure in which many servers across the Internet maintain a distributed database of hostname-to-IP mappings. DNS servers maintain hostname-to-IP mappings for their zone. If a DNS server receives a request for DNS resolution of a domain outside its zone, the DNS server forwards the request to another DNS server within the requested zone. The following three components comprise the domain naming system:

- **Resource records and domain namespace:** The domain namespace is the naming used to organize the resource records in a hierarchical format. Resource records identify the type of host, IP address, or a parameter of the DNS database.
- **Domain name servers:** These servers store resource records in a database and maintain information about the domain namespace structure. A DNS server, using its database, resolves requests for its zone and forwards outside requests to additional predefined DNS servers.
- **Resolvers:** Applications or a part of the operating system that queries a DNS server. DNS clients use resolvers to query a DNS server, and DNS servers use a resolver to forward queries to other DNS servers.

The hierarchy of the domain name system begins at the top with top-level domains such as .com, .gov, .mil, and .org. Top-level domains can also represent countries such as .jp, .us, and .uk; in the absence of a specific country code, .us is the default, if unseen, code. These top-level domains are followed by second-level domains such as cisco, cia, and navy. Yet another level exists to define a specific location within second-level domains such as mail, web, or public. For example, a request to a local DNS server on your network for mail.cisco.com causes the local DNS server to forward the request to cisco.com, where Cisco's DNS servers can respond with the location of mail.cisco.com. A domain that points to a specific computer in a domain is considered a fully qualified domain name (FQDN). If mail.cisco.com points to a mail server at mail.cisco.com, it is an FQDN.

7.3.3: The following steps occur when a host wants to resolve a DNS name such as mail.cisco.com:

1. The host uses a resolver to query a DNS server inside its domain for the IP address of mail.cisco.com. This DNS server is preconfigured for the host.
2. The DNS server receives the request and checks its local records. If the DNS server cannot resolve the domain name, it forwards the request to another preconfigured DNS server. The local DNS server may query a root DNS server to discover the location of top-level .com domain name servers.
3. The top-level DNS server, after being queried, responds with the location of the cisco.com DNS server for the requested domain.
4. The local DNS server then queries the cisco.com DNS server for the location of mail.cisco.com. When the resolved name to IP address is returned, each DNS server caches the record for a limited amount of time.
5. The local DNS server receives the returned request, temporarily caches the record, and responds to the requesting host with the IP address for mail.cisco.com.

Because of the widespread use of Dynamic Host Configuration Protocol (DHCP) to assign addresses and names to hosts, a host on a DHCP network can dynamically register its record with a DNS server on the same network. Dynamic updates, however, are not enabled by default.

DNS zones can be broken into primary or secondary forward lookup or reverse lookup zones:

- **Forward lookup zones:** The standard zone that resolves FQDNs to IP addresses. An example of this process is when a browser sends a recursive query to the local DNS server for www.cisco.com to determine the IP address.
- **Reverse lookup zones:** This query works in reverse: A host knows the IP address and requests the FQDN. Private networks use reverse lookup to identify host names on their local network. Some applications also use reverse lookup to identify the hostname from the IP address of a computer communicating from the Internet.
- **Primary and secondary:** There can be primary and secondary forward lookup and reverse lookup zones. The primary zone is where you update records, and the secondary zone operates as a read-only backup copy of the primary zone.

7.3.4: You can use the DNS servers from your ISP or run your own DNS servers. Table 17-1 identifies the key points of both implementations.

Table 17-1 ISP and Local DNS Servers

ISP DNS Servers	Local DNS Servers
Typically caching-only servers configured to send all resolution requests to root servers in the Internet	Can store authoritative name-to-IP mappings in their database
The large number of requests creates a large cache of DNS lookups	Can be configured to forward requests directly to the root DNS server
Typically do not store authoritative name-to-IP mappings in their database	Also can be configured to forward queries to the ISP DNS server to benefit from the larger cache of DNS lookups

You might want to use redundant DNS servers to provide fault tolerance in case a primary DNS server fails.

Summary

The process that computers use to translate a meaningful domain name to an IP address allows users to better use and understand services available on a network. DNS becomes even more important with the advent of IPv6 and 128-bit hexadecimal addresses. The operation of DNS and the tools mentioned today allow you as an administrator to better troubleshoot DNS-related issues. You can review TCP/IP and DNS on pages 39–68 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 16

Describe the Operation and Benefits of Using Private and Public IP Addressing

Many claim that the introduction of private addressing saved the world from an imminent shortage of IP version 4 addresses. However, as a result of the widespread implementation of private addressing, many home users believe their public address to be 192.168.1.2. You will have the knowledge to set these users straight after you review Chapter 5 of *CCNA Discovery 1*.

CCNA Discovery 1, Chapter 5

5.2.2: On Days 20 and 18 we discussed private addressing in reference to network address translation (NAT) and IP addressing. The following key points summarize the operation and benefits of public and private addressing:

- A device directly connected to the Internet has a public IP address. This address is routable, and other devices on the Internet can identify, locate, and request services from a device that has a public IP address.
- The number of public IP addresses is limited, so RFC 1918 reserved Class A, B, and C networks for private use on an internal network. These address ranges can be reused for multiple internal networks because the networks are not visible to the Internet or each other.
- A router running NAT and PAT can allow devices on a private network to share a single public IP address and communicate over the Internet.
- Devices on a private network behind a router running NAT are not directly accessible on the Internet, providing additional security.
- RFC 1918 reserves one Class A address for private networks: 10.0.0.0. This network allows more than 16 million private addresses.
- RFC 1918 reserves 16 Class B networks for private use: 172.16.0.0 to 172.31.0.0. Each network allows more than 65,000 private addresses.
- RFC 1918 reserves 256 Class C networks for private use: 192.168.0.0 to 192.168.255.0. Each network allows up to 254 private addresses.

Enable NAT for a Small Network with a Single ISP and Connection Using SDM, and Verify Operation Using CLI and Ping

On Day 18 we discussed NAT operation and looked at the CLI configuration for NAT. Today we look at a graphical way to configure NAT as well as some tools you can use to verify NAT operation on your network. Chapter 5 of *CCNA Discovery 2* covers this material.

CCNA Discovery 2, Chapter 5

5.2.1 and 5.2.2: Cisco SDM Express is a graphical tool that allows you to quickly create a basic configuration on a router. Cisco SDM Express allows you to set a hostname, domain name, login information, interface addressing, and protocols such as DNS and DHCP. As with most graphical configuration interfaces, you need to understand the protocols and terminology to correctly fill in the forms.

5.2.4 and 5.2.5: Cisco SDM Express allows you to complete a basic configuration, but Cisco SDM provides a more advanced interface. The Cisco SDM basic NAT wizard allows you to configure basic or advanced NAT on your router. After you launch the NAT wizard in the graphical user interface (GUI), you need to choose the interface connected to the Internet and the internal IP address range. The following steps provide a basic overview of NAT configuration using PAT with Cisco SDM:

Step 1 Connect one port on the router to an external network and one port to a private network.

Step 2 Connect a PC to an Ethernet port on the router, and assign the address 192.168.1.2 to the PC. Check connectivity LEDs, and then open a web browser on the PC and navigate to the address http://192.168.1.1.

Step 3 Complete a basic configuration on the router, including proper interface addresses, hostname, usernames, and passwords.

Step 4 From the Configure menu in Cisco SDM, choose Basic NAT, and launch the task.

Step 5 Follow the wizard, and select the WAN interface connected to the outside network or ISP.

Step 6 Choose the range of internal addresses for the hosts on your private network that you would like to share with the outside connection.

Step 7 Complete the wizard. Be sure to check the box that saves the running configuration.

Step 8 Revisit the Configure menu. Navigate to the Edit NAT Configuration tab to verify the inside and outside interface and proper address translation.

Step 9 Connect the serial port of the PC to the console port on the router, and open a terminal. Turn on ICMP debugging with the command **debug ip icmp**. Keep the terminal window visible, and open a command prompt on the PC as well.

Step 10 From the PC command prompt, ping an address on the external network, and watch the terminal's output to verify proper NAT operation.

Summary

The concepts of private and public IP addressing tie in directly to the proper configuration of NAT. The purpose of NAT is to translate between private networks and the public Internet. Many users with NAT enabled see no difference in the connection and surf as if they have a public IP address. It is your job as an administrator to ensure that NAT operates seamlessly and to troubleshoot any issues for these users. You can further review the topics from today on pages 39–68 and 255–292 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 15

Configure, Verify, and Troubleshoot DHCP and DNS Operation on a Router (Including CLI/SDM)

Hosts on your network can obtain address and DNS information automatically if you have enabled Dynamic Host Configuration Protocol (DHCP). Chapter 5 of *CCNA Discovery 1* discusses the operation of DHCP. Chapter 5 of *CCNA Discovery 2* explains how to configure DHCP, including important parameters for DNS.

CCNA Discovery 1, Chapter 5

5.3.2: You can manually enter the IP address on a host, or a host can dynamically acquire the address through DHCP. Typically, a DHCP client requests addressing information from a DHCP server on a network. A PC acts as a DHCP client for an integrated services router (ISR), and the ISR can act as a DHCP client for the ISP.

5.3.3: A client that needs an IP address completes the following steps to obtain an IP address on a DHCP network:

1. The client sends a **DHCP Discover** message with a destination IP address of 255.255.255.255 and a destination MAC address of FF-FF-FF-FF-FF-FF.

2. This DHCP Discover message broadcasts over the network, and the DHCP server replies with a **DHCP Offer**, including a suggested IP address.

3. The requesting client sends a **DHCP Request** to use the IP address suggested in the DHCP offer.

4. The DHCP server responds with a **DHCP Acknowledgment**.

A DHCP server can provide addresses to a host on a different network if the routers on those networks are configured to forward DHCP requests with the **ip helper-address** command.

In a graphical interface on a router (including SDM), you can enable DHCP and set parameters such as the start IP address, maximum number of users, client lease time, and IP address range for DHCP. In addition, an ISR allows you to view client lease times, IP addresses, and MAC addresses in a DHCP client table.

CCNA Discovery 2, Chapter 5

5.3.7: The following commands allow you to use the Cisco IOS CLI to configure a router to function as a DHCP server:

```
ip dhcp pool pool-name
network network-address subnet-mask
domain-name domain-name
dns-server dns-server-address
default-router default-router-address
lease {days [hours] [minutes] ¦ infinite}
```

For example:

```
Router> enable
Router# configure terminal
Router(config)# ip dhcp pool LAN-three
Router(dhcp-config)# network 192.168.3.0 255.255.255.0
Router(dhcp-config)# domain-name cisco.com
Router(dhcp-config)# dns-server 192.168.3.2
Router(dhcp-config)# default-router 192.168.3.254
Router(dhcp-config)# lease infinite
```

You can use the following commands to exclude a range of addresses or a single address from the DHCP pool that you want to reserve and assign to specific hosts from global configuration mode:

```
ip dhcp excluded-address start-address end-address
ip dhcp excluded-address single-address
```

For example:

```
Router(config)# ip dhcp pool excluded-address 192.168.3.1 192.168.3.20
Router(config)# ip dhcp pool excluded-address 192.168.3.254
```

To verify that DHCP is operating and to check the configuration, use the following commands. Make sure that you test all **show** commands in a lab or simulation so that you are familiar with the output.

```
show running-config
show ip dhcp binding
show ip dhcp server statistics
debug ip dhcp server events
```

You can start and stop the DHCP service with these two commands:

```
service dhcp
no service dhcp
```

Summary

DHCP provides a way to centralize address assignment and ensure that all devices on a network receive the proper address information. Network administrators often combine DHCP and DNS configurations with NAT to implement a fully functioning, efficient, manageable, scalable network. You can further review DHCP configuration on pages 219–250 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 14

Implement Static and Dynamic Addressing Services for Hosts in a LAN Environment

Hidden in today's topic are many of the topics covered on previous days. Included in address implementation is the underlying concept of IP addressing and the protocols that support address assignment and translation, such as DHCP and NAT. Chapters 2 and 5 of *CCNA Discovery 1* discuss the general ideas behind address implementation to consider when implementing IP addressing, Dynamic Host Configuration Protocol (DHCP), and Network Address Translation (NAT).

CCNA Discovery 1, Chapter 2

2.2.3 and 2.2.4: You can assign an address to hosts in your LAN in one of the following ways:

- **Manual configuration:** You can enter a static IP address, subnet mask, and gateway on hosts in your network. These static addresses remain the same for these devices unless you manually change them.
- **Dynamic configuration:** You can configure a DHCP server to dynamically assign addresses to computers on your network. You can specify the address range, client lease, and other parameters on the DHCP server. You also need to configure clients to request addressing information from the DHCP server.

You can also provide each host with a unique network name to aid in troubleshooting and identification on the network.

CCNA Discovery 1, Chapter 5

5.3.1: Consider the following key points when implementing static and dynamic services on your LAN:

- Devices on your LAN that other computers and applications share and access for services should have static IP addresses. For example, a local web server or printer should always have the same static IP address on a LAN.
- Desktops and mobile clients that only access services and do not host services on a network should obtain IP addresses dynamically to allow for mobility and scalability of the network.
- You have better control over a small network with static address assignment; however, static addressing is more time-consuming and increases the possibility of duplicate IP addresses.

Summary

The best way to review address service implementation is to actually design and implement an addressing scheme on a network. Today's short topic lets you implement on a real network the theory you have learned about network addressing. If you do not have a real network available, open Packet Tracer and build an impressive network that includes subnetworks, variable-length subnet masking (VLSM), Classless Interdomain Routing (CIDR), DHCP, and NAT. You can test your understanding of IP addressing on pages 39–68 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 13

Identify and Correct IP Addressing Issues

IP addresses are complex and involve numerous numbers and dots. Sometimes an IP address or subnet mask is entered incorrectly, and it takes a sharp-eyed network admin to recognize the issue and save the day. Chapter 9 of *CCNA Discovery 1* and Chapter 2 of *CCNA Discovery 2* identify methods you can use to identify and correct IP addressing issues.

CCNA Discovery 1, Chapter 9

9.2.4: You can cut right to Layer 3 and troubleshoot connectivity with **ping**. If the ping is successful, you have an upper-layer issue, and the IP addressing is OK for your host. An unsuccessful ping using a domain name followed by a successful ping using an IP address indicates an issue with DNS.

9.3.6: If your computer is configured to obtain an IP address automatically, you can follow these steps to check DHCP operation on a PC running Windows:

Step 1 Check the IP configuration on your host; open a command prompt and enter the command **ipconfig /all**. Look at the subnet mask, gateway, DNS settings, and IP address.

Step 2 Make sure that the gateway and host IP addresses are on the same subnet.

Step 3 Try releasing and renewing the dynamic IP address with the commands **ipconfig /release** and **ipconfig /renew**.

9.3.7: A successful ping to your gateway router followed by an unsuccessful ping to an Internet address indicates a problem with your connection between the router and the ISP. You can first check that your router has a public IP address and a proper configuration to communicate with the ISP. You may have to contact the ISP to troubleshoot the connection to its network.

CCNA Discovery 2, Chapter 2

2.2.3: When you check the IP address configuration on a device, it is important to consider all the aspects of an IP addressing scheme, as covered on Day 20. Look for simple address entry errors as well as incorrect subnet mask, gateway, or DNS settings. You can use **traceroute** in addition to **ping** and **ipconfig** to troubleshoot the configuration and connectivity of network devices.

Summary

The tools provided today allow you to view and renew IP addresses. However, you need a solid understanding of IP addressing and subnetting to recognize complex IP addressing issues. The best practice for IP address troubleshooting is to create a network and then have someone create issues for you to solve. You can do this with a real network or a simulated one in Packet Tracer. Either way, just do it. You can further review IP connectivity troubleshooting on pages 71–84 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Part IV

Days 12–8: Implement a small routed network

Day 12 covers routing and routers

Day 11 covers RIP configuration

Day 10 covers CLI parameters

Day 9 covers configuration, IOS, and security

Day 8 covers network status verification

Describe Basic Routing Concepts (Packet Forwarding, Router Lookup Process)

Routers see networks, not hosts. Routers are a little like a taxi driver in New York. If you tell the driver to take you to room 201 of the Empire State Building, he or she will ignore the room number and take you to the building. Similarly, a router looks at a destination network, not the specified host portion of a destination address. Chapter 6 of *CCNA Discovery 2* covers the concepts behind how a router learns about destination networks to forward a packet to its intended destination.

CCNA Discovery 2, Chapter 6

6.1.1: Routers decide where to forward a packet by using information stored in routing tables. A router maintains a list of its interfaces and which networks are connected to those interfaces in its routing table. You can manually add a static route to a routing table, or routers can dynamically learn about routes from other routers, using a routing protocol. The following key points define the process a router uses to forward a packet:

1. A packet arrives at the router containing a destination IP address and subnet mask. The router uses the subnet mask to determine the packet's network bits and destination network.
2. The router references its routing table to find an entry with a matching destination network. In addition, the router looks at the route cost of each matching route to find the shortest path.
3. The matching route in the table identifies the network interface associated with the destination network, so the router forwards the packet out that interface to the next hop.
4. If there are no routes with matching destination networks, the router forwards the packet to a manually configured default route.

Table 12-1 defines four types of routes that exist in a routing table.

Table 12-1 Routes in the Routing Table

Route Type	Features
Directly connected	The router detects configured networks connected to its interfaces and adds them to the routing table automatically. These routes are identified by the prefix *C*. They automatically update when the configuration changes or an interface is shut down.
Static	This is a manually configured route added by the administrator and identified by the prefix *S*.

continues

Table 12-1 Routes in the Routing Table *continued*

Route Type	Features
Dynamic	Routers use routing protocols to communicate information about routes in their routing table. These routes are dynamically updated by the routing protocol, and the prefix for a dynamic route is based on the type of protocol. For example, Routing Information Protocol (RIP) is identified by the prefix *R*.
Default	An administrator configures a static route that identifies the default gateway for packets with a destination network a router does not have in its routing table.

6.1.2 and 6.1.3: A small network with few routers may function properly with manually configured static routes. However, larger networks can update quickly and adapt to network changes without administrators through the use of dynamic routing. Dynamic routing protocols typically use one of the two algorithms defined in Table 12-2.

Table 12-2 Routing Algorithms

Distance Vector	Link-State
Periodically exchanges routing tables with neighboring routers.	Exchanges link-state advertisements (LSA) across the network to update routing tables when a change occurs in a link on the network.
Evaluates routes based on a network's distance (how far) and vector (what direction).	Maintains a topological database of the network and builds a shortest path first (SPF) tree to represent the network, with the router at the top.
Distance is expressed in a route cost or metric including hops, administrative cost bandwidth, transmission speed, likelihood of delays, and reliability.	Each time an LSA is received, the router updates and recalculates paths with the SPF algorithm.
A router receives the routing table from a neighbor, updates its routing information, and forwards its routing table with an added hop to neighboring routers.	

Routing Information Protocol (RIP) is a simple distance vector protocol used on small and medium-sized networks. The following are the key characteristics and disadvantages of RIP:

- Routers using RIP exchange complete copies of their routing table with neighbors and allow a maximum hop count of only 15 routes.
- The periodic exchange of routing tables can increase network traffic, and it can take a long time for routers to learn about all routes on a network (converge).
- RIP uses the hop count to determine the best path across a network.
- RIP version 2 (RIPv2) is preferred over RIP version 1 because RIPv2 includes subnet mask information in routes, whereas RIP version 1 relies on classful default subnet masks. Therefore, RIPv2 allows variable-length subnet masking (VLSM) and Classless Interdomain Routing (CIDR).

Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior routing protocol with features beyond the capabilities of RIP. EIGRP is a Cisco-proprietary routing protocol with the following characteristics:

- EIGRP uses hop count as well as metrics such as bandwidth and delay to calculate the best path. EIGRP has a maximum hop count of 224. The five possible factors in the EIGRP metric are bandwidth, delay, load, reliability, and maximum transmission unit (MTU).
- In addition to the routing table, EIGRP maintains a neighbor table and topology table.
- EIGRP uses advertisements from neighboring routers to build a topology table and then uses the Diffused Update Algorithm (DUAL) to calculate the best path.
- With advertisements and the DUAL algorithm, EIGRP is an enhanced distance vector routing protocol that converges more quickly than RIP.

Open Shortest Path First (OSPF) is a nonproprietary interior routing protocol. The following points characterize OSPF:

- OSPF is a link-state routing protocol that sends link state advertisement (LSA) routing updates when a topology change occurs on the network.
- OSPF supports VLSM, CIDR, and route authentication.
- OSPF uses the shortest path first (SPF) algorithm to calculate the lowest-cost route and maintain an SPF tree.

6.1.4: A smaller network can function properly with static routes or a simple interior routing protocol such as RIP. However, as the number of routers in a network increases, a more advanced routing protocol such as EIGRP or OSPF can more efficiently update the routing tables and allow the network to quickly converge.

Describe the Operation of Cisco Routers (Router Bootup Process, POST, Router Components)

As the engine that directs traffic across networks, the router uses a complex combination of hardware and software. Chapter 5 of *CCNA Discovery 2* describes how a router becomes operational when you flip the power switch.

CCNA Discovery 2, Chapter 5

5.1.4–5.1.6: Cisco IOS software allows you to configure the router from a command-line interface (CLI). You can also use the Cisco Router and Security Device Manager (Cisco SDM) as a graphical user interface (GUI) to configure the router. When you first power on the router, it performs the following tasks in addition to loading Cisco IOS software:

1. The router performs a power-on self-test (POST) to check its hardware.
2. The router loads a bootstrap and initializes the Cisco IOS image from flash, a TFTP server, or read-only memory (ROM). The location of the Cisco IOS image is usually specified in the configuration register.
3. After the IOS image is loaded, the router loads the startup configuration file from nonvolatile random-access memory (NVRAM) to random-access memory (RAM) as the running configuration.
4. If NVRAM has no configuration file, the router searches for a TFTP server with the configuration file. As a last resort, it starts the setup dialog.
5. As soon as the router is up and running, the terminal displays the user EXEC prompt **router>**, and the router is ready for you to configure its interfaces and other parameters.

Each time after you configure the router, it is important to execute the command **copy running-config startup-config** to ensure that the router saves the new configuration in NVRAM and will initialize the new configuration when restarted.

Select the Appropriate Media, Cables, Ports, and Connectors to Connect Routers to Other Network Devices and Hosts

A router with no cables is like an octopus without arms: sad. Chapter 5 of *CCNA Discovery 2* describes the various arms available for your router.

CCNA Discovery 2, Chapter 5

5.1.1–5.1.3: The following ports and slots appear on the back of a Cisco 1841 integrated services router (ISR):

- High-Speed Wide-Area Network Interface Card (HWIC) slots support serial connectivity over a wide-area network (WAN).
- A compact flash module allows the use of compact flash memory to store software for router operation.
- A USB flash port allows router software and configurations to be stored directly to USB flash memory.
- Fast Ethernet ports provide 10\100 Mbps connectivity for the router. When a local-area network (LAN) connection is activated, you can connect to the router in-band over Telnet or HTTP to make configuration changes.
- A console port allows you to connect the router directly to a PC with an RJ-45-to-DB-9 console cable and use terminal emulation software to perform out-of-band router management. Out-of-band management does not require an active LAN connection.

- An AUX port allows you to configure the router using a modem for out-of-band management.
- An ISR can also include a four-port Ethernet switch to allow you to connect local devices on the LAN.
- A power port for a standard power cord.

Summary

Today you reviewed a router's physical connections, startup process, and basic software operation—in essence, the heart and soul of internetwork communications. When somebody asks you how data gets from her home to a server, you can now provide a one-word answer: routers. If she needs more information, read her this chapter. We will discuss WAN connectivity more on Day 3. You can further review the topics from today on pages 192–216 and 219–250 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 11

Configure, Verify, and Troubleshoot RIPv2

RIP version 2 (RIPv2) allows a router to discover the location of remote networks dynamically from other routers running RIPv2. Chapter 6 of *CCNA Discovery 2* provides the steps necessary to configure, verify, and troubleshoot RIPv2.

CCNA Discovery 2, Chapter 6

6.1.5: To configure RIPv2 on a network, follow these steps:

Step 1 Physically connect the routers, power up each router, and check the LEDs to ensure connectivity.

Step 2 Plan an IP addressing scheme that provides sufficient addresses for all networks connected to each router.

Step 3 Connect to each router with a console cable (out-of-band management), configure the proper IP address, and activate each interface.

Step 4 Determine which networks are directly connected to each router, and use RIP to configure that router to advertise the location of those networks.

The following commands allow you to enable RIP on a router directly connected to a specific network:

```
router rip
version 2
network directly-connected-network
```

For example, the following commands allow you to enable RIP on a router directly connected to the networks 192.168.1.0, 192.168.2.0, and 172.16.0.0:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 172.16.0.0
```

Table 11-1 describes the commands you can use to verify your RIPv2 configuration and operation.

Table 11-1 Commands to Verify RIPv2

Command	Description
ping	Tests connectivity to remote networks across routers.
show ip route	Displays all routes in the routing table and indicates routes learned through RIPv2 using the prefix *R*.
show ip protocols	Verifies that RIPv2 is configured and operating on the router and that the router is receiving updates and advertising routes.
debug ip rip	Displays RIP advertisements on the network in real time. This command is processor-intensive, so it should be turned off with the **undebug all** command after use.
show running-config	Displays the router configuration, including RIP commands and networks the router is advertising.
show interfaces	Displays interface configurations so that you can check that the interface IP address is part of its advertised networks.

Summary

First you enter **router rip**, and then you enter **version 2**, and finally you enter **network** followed by the directly connected networks. After that, the routers on your network do the rest to build routing tables and get packets from destination to destination. You can watch the fun (at the processor's expense) in real time using the command **debug ip rip**. You can further review the topics from today on pages 295–312 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 10

Access and Use the Router CLI to Set Basic Parameters

Your users may judge you by how well your network runs, but other network administrators will judge you by your skills at the command-line interface (CLI). Do not be fooled by these fancy graphical interfaces that may entice you to configure using their pretty checkboxes and multiwindowed wizards. The real network wizards need no graphics; a simple prompt and keyboard can get the job done and prove your value in the hierarchy of network admins. Chapter 5 of *CCNA Discovery 2* covers the basics of the CLI on a router.

CCNA Discovery 2, Chapter 5

5.3.1: As discussed on Day 23 for the switch, the Cisco IOS CLI provides the following command modes:

- **User EXEC** mode is the default mode, where you can view information about the operation of a switch and test connectivity.
- **Privileged EXEC** mode allows you to adjust the router's operation and view configuration files.
- **Global configuration** mode allows you to configure the router and enter submodes for specific configurations.

5.3.2: If you enter the **help** command at the command prompt, the Cisco CLI describes the help system. You can also use the question mark for additional help in the following ways:

- If you enter the first few letters of a command with a question mark at the end (no space), the output lists all possible commands for that mode beginning with those letters.
- You can enter the first word of a command string followed by a space and then a question mark to view the possible options for that command.
- If you enter a command incorrectly and the ^ symbol identifies the beginning of your error, you can enter the letters up to that point followed by a question mark to view any possible commands. Try the question mark with and without a space to determine all possible options.

Table 10-1 describes helpful commands and keystrokes for the Cisco CLI.

Table 10-1 Helpful Commands and Keystrokes for the Cisco CLI

Command or Keystroke	Description
terminal history size	Allows you to change the number of commands recorded during a terminal session. The default is ten.
Ctrl-P or the up arrow	Allows you to recall recent commands.

continues

Table 10-1 Helpful Commands and Keystrokes for the Cisco CLI *continued*

Command or Keystroke	Description
Ctrl-N or the down arrow with the up arrow.	Allows you to navigate back through recalled commands accessed
Tab key	Completes a partially entered command.

5.3.4: After configuring a device, always remember to copy the running configuration to the startup configuration. The following commands demonstrate the basic configuration for a router:

```
Router> enable
Router# configure terminal
Router(config)# hostname RouterA
RouterA(config)# banner motd #
Enter TEXT message. End with the character '#'.
Welcome to RouterA
#
RouterA(config)# enable password ciscopass
RouterA(config)# enable secret class
RouterA(config)# line console 0
RouterA(config-line)# password cisco
RouterA(config-line)# login
RouterA(config-line)# exit
RouterA(config)# line vty 0 4
RouterA(config-line)# password cisco
RouterA(config-line)# login
RouterA(config-line)# exit
RouterA(config)# service password-encryption
RouterA(config)# exit
RouterA# copy running-config startup-config
```

Connect, Configure, and Verify the Operation Status of a Device Interface

I like to imagine packets piling up at the end of the cable, just waiting to be accepted by the router. They wait for you to activate and assign an IP address to the interface so that the router can start business for the day. Chapter 5 of *CCNA Discovery 2* describes the steps necessary to configure a serial and Ethernet interface on a router.

CCNA Discovery 2, Chapter 5

5.3.5: The following examples provide the basic commands to configure an Ethernet and serial interface on a router. If the serial interface is a data communications equipment (DCE) device, you need to set the clock rate. However, a router is more often the data terminal equipment (DTE) device, and you do not set a clock rate for a DTE device interface. As a DTE, the router would accept the clock rate from a DCE device.

The following is a sample configuration for a router Ethernet interface:

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# interface fa0/0
RouterA(config-if)# ip address 192.168.1.1 255.255.255.0
RouterA(config-if)# description Main Office LAN
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# ip host RouterA 192.168.1.1
RouterA(config)# exit
RouterA# copy running-config startup-config
```

The following is a sample configuration for a router DCE serial interface:

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# interface serial 0/0
RouterA(config-if)# description Connection to RouterB
RouterA(config-if)# ip address 192.168.2.5 255.255.255.252
RouterA(config-if)# clock rate 64000
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# exit
RouterA# copy running-config startup-config
```

The following commands allow you to verify your interface configuration:

```
show running-config
show interfaces
show ip interface brief
```

Verify Device Configuration and Network Connectivity Using ping, traceroute, Telnet, SSH, or Other Utilities

Utilities such as ping and traceroute will surface and resurface throughout your career as you troubleshoot networks. These utilities allow you to check connectivity on a network, or discover that the problem is outside your administrative reach. Chapter 5 of *CCNA Discovery 2* covers the **ping** and **traceroute** commands.

CCNA Discovery 2, Chapter 5

5.3.5: You can verify connectivity between routers and networks with the **ping** command. In addition, the following example shows how to enable Telnet, SSH, and the HTTP server on your router for additional connectivity verification (when SDM is not already enabled).

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# ip http server
RouterA(config)# ip http secure-server
RouterA(config)# username cisco privilege 15 password 0 class
RouterA(config)# line vty 0 4
RouterA(config-line)# privilege level 15
RouterA(config-line)# login local
RouterA(config-line)# transport input telent
RouterA(config-line)# transport input telnet ssh
RouterA(config-line)# exit
```

After you have enabled the web server, Telnet, and SSH, you can test connectivity by entering the router’s address in a web browser or by using the **ssh** or **telnet** commands to access the router from another router. If you are unsure about the use of these commands, you can always enter the command followed by a space and a question mark to view your options.

Summary

As your comfort level with the CLI for configuration and verification increases, so does your ability to efficiently and masterfully adapt and prepare your network for your beloved users. Never miss an opportunity to open a terminal and enter these impressive CLI commands in front of a supervisor or fellow technician. You can further review the topics from today on pages 219–250 of *CCNA Flash Cards and Exam Practice Pack* (CCENT Exam 640-822 and CCNA Exams 640-816 and 640-802), Third Edition.

Your Notes

Day 9

Perform and Verify Routing Configuration Tasks for a Static or Default Route Given Specific Routing Requirements

Sometimes you simply need to configure a router with specific routes for a small network. You can use static and default routes for situations in which you do not want to use a dynamic routing protocol. Chapters 5 and 6 of *CCNA Discovery 2* provide the commands necessary to configure a default or static route.

CCNA Discovery 2, Chapter 5

5.3.6: Any packets for which a router does not know the destination are forwarded to the default route. Use the following command to set a default route:

```
ip route 0.0.0.0 0.0.0.0 {outgoing-interface ¦ next-hop-address}
```

For example (using the outgoing interface):

```
Router(config)# ip route 0.0.0.0 0.0.0.0 s0
```

CCNA Discovery 2, Chapter 6

6.1.1: Static routes are identified with the prefix *S* in the routing table and can be changed only with manual configuration. You can manually configure a static route with the following command:

```
ip route destination-network subnet-mask {outgoing-interface ¦ next-hop-
  address}
```

For example (using the next-hop-address):

```
Router(config)# ip route 192.168.4.0 255.255.255.0 192.168.3.2
```

You can verify default and static routes with the following commands:

```
show running-config
show ip route
```

Manage IOS Configuration Files (Save, Edit, Upgrade, Restore)

You can always restore your router to an earlier configuration if you have periodically saved your router configurations to a server on your network. Chapter 5 of *CCNA Discovery 2* outlines the steps necessary to back up and restore your IOS configuration files.

CCNA Discovery 2, Chapter 5

5.3.9: If you have a trivial file transfer protocol (TFTP) server on your network, you can use the following commands on a router to back up the running configuration file to the TFTP server:

```
copy running-config tftp
{enter host IP address}
{type a name for the configuration file}
{type y}
```

For example:

```
Router# copy running-config tftp
Address or name of remote host []? 10.0.0.25
Destination filename[router-config]? portland.1
Write file portland.1 to 10.0.0.25 [confirm] y
Writing Portland.1 !!!!!! [ok]
```

To restore the file to your router, use the following commands:

```
copy tftp running-config
{select a host or network configuration file}
{enter host IP address}
{type the name of the configuration file}
{type y}
```

For example, to restore a backup configuration from a TFTP server, you might enter the following:

```
Router# copy tftp running-config
Address or name of remote host []? 10.0.0.25
Source filename []? portland.1
Destination filename [running-config]? running-config
Accessing tftp://10.0.0.25/portland.1
!!!!!!!!!!!!!
752 bytes copied in 8.03 secs
Router#
```

You can also copy the output of the **show running-config** command from your terminal and paste it into a text file to back up a configuration.

Manage Cisco IOS

Chapter 5 of *CCNA Discovery 2* identifies the function of IOS. The following section expands on this discussion and adds the basic commands necessary to locate, back up, and restore the Cisco IOS software.

CCNA Discovery 2, Chapter 5

5.1.4: Cisco IOS software provides the underlying support for router operation and configuration tools such as the command-line interface and the Cisco router and security device manager (SDM). The **show version** command allows you to check the image name of the IOS image on your router. Use the **copy flash tftp** command to copy the IOS image from your router's flash memory to a TFTP server. To restore a backup IOS image from a TFTP server to flash memory, use the command **copy tftp flash**.

Implement Password and Physical Security

Your network is more secure if you plan to restrict physical as well as electronic access to your routers and networking equipment. Chapters 3 and 5 of *CCNA Discovery 2* provide physical considerations and configuration commands you may use to better secure your network and networking equipment.

CCNA Discovery 2, Chapter 3

3.2.2: It is important to secure the telecommunications room or wiring closets in your facility. The main distribution facility (MDF) and intermediate distribution facilities (IDF) are the backbone of the network and should be protected. Access to these areas should be restricted to staff members who maintain and understand the equipment.

CCNA Discovery 2, Chapter 5

5.3.4: As covered on Day 10, it is important to protect configuration privileges in the Cisco IOS software on a router or switch by adding password security. You should set a password for privileged EXEC mode, console access, and virtual terminal access. Keep in mind that if the enable password and enable secret password are both set, the secret overrides the enable. The following example adds password security and encrypted password security for privileged EXEC mode on a router:

```
Router> enable
Router# configure terminal
Router(config)# enable password ciscopass
Router(config)# enable secret class
```

To add password security for console access and virtual terminal access to a router, you would enter the following:

```
Router> enable
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exit
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exit
```

You can ensure that passwords are encrypted if you enter the command **service password encryption** in global configuration mode. In addition, do not forget to copy the running configuration to the startup configuration with the command **copy running-config startup config**.

Summary

Default routes, backup policies, passwords, and locked doors improve security on your network. Network security is important to protect your investment in equipment and the time it takes to build a functioning network. Each of these factors should be documented and implemented in the early stages of network planning and design.

Your Notes

Day 8

Verify Network Status and Router Operation Using Basic Utilities (ping, traceroute, Telnet, SSH, ARP, ipconfig, show, and debug Commands)

Day 8 looks a lot like Day 10; however, at this point in your review you have completely covered router and switch configurations and operation topics. While you quickly review the network verification utilities described in Chapter 9 of *CCNA Discovery 1* and Chapters 5 and 6 of *CCNA Discovery 2*, consider how you might use these tools to maintain a fully configured network.

CCNA Discovery 1, Chapter 9

9.2.3–9.2.7: You can use software utilities on network hosts as well as routers and switches to test and monitor connectivity. The following utilities allow you to troubleshoot network issues:

- **ipconfig:** This utility allows you to view the IP configuration on a host running Windows and compare the configuration to your router's network configuration.
- **ping:** Both network devices and network hosts allow you to test Layer 3 connectivity and basic DNS functionality with ping.
- **tracert or traceroute:** This utility allows you to view each hop a packet encounters on the way to its destination. **tracert** is the command for a windows host, and **traceroute** is the command for the router CLI.
- **netstat:** You can view information about devices communicating with a host, including IP address and TCP port information.
- **nslookup:** This command on a host allows you to troubleshoot DNS resolution on your network.

CCNA Discovery 2, Chapter 5

5.3.3: Table 8-1 describes common **show** commands that a network administrator may use to verify the configuration and operation of a router.

Table 8-1 Common Cisco IOS Software show Commands

Command	Description
show running-config	Displays the running configuration from RAM on the router.
show interfaces	Displays information about the router interfaces, including encapsulation, address configuration, and whether the interface is up or down.
show arp	Displays any Address Resolution Protocol (ARP) entries learned by the router.
show ip route	Displays routes manually configured or dynamically discovered by the router.
show users	Displays any users connected to the router.
show version	Displays the version of Cisco IOS software running on the router, the name of the image, and the amount of RAM.

5.3.5: After you have configured a routing protocol, interface addresses, and remote login (including SDM) on a router, you can test Layer 7 connectivity by accessing the router through SSH, Telnet, and a web browser using a host on your network.

CCNA Discovery 2, Chapter 6

6.1.5: You can tell a router to output additional information about network operation with the **debug** command. For example, the command **debug ip rip** outputs all RIP updates a router sends and receives in real time. You can enter a question mark with a space after the **debug** command to see additional options. Keep in mind that debugging puts a heavy load on the router processor, so it is important to execute the **undebug all** command to turn off debugging when you are finished.

Summary

Now that you have completed the CCENT topics of IP addressing, switch configuration, router configuration, and troubleshooting, you should practice building and troubleshooting networks. If you do not have access to a lab, Packet Tracer allows you to simulate the scenarios and issues you might encounter on the exam. Spend some time building and debugging the most complex network you can design.

Your Notes

Part V

Days 7–6: Explain and select the appropriate administrative tasks required for a WLAN

Day 7 covers wireless standards

Day 6 covers wireless security

Describe Standards Associated with Wireless Media (Including the IEEE Wi-Fi Alliance and ITU/FCC)

Wireless works where cables don't. Today you will review the capabilities and limitations of wireless LANs (WLAN). The frequencies, network classifications, and standards of a WLAN are covered in Chapter 7 of *CCNA Discovery 1*.

CCNA Discovery 1, Chapter 7

7.1.1: Wireless devices use electromagnetic waves as the physical media for data transmission. Whereas infrared (IR) can transmit data over short distances, radio frequency (RF) waves are capable of distances and speeds necessary for networking. The following RF bands are used by unlicensed devices for communication. These bands are called the Industrial, Scientific, and Medical (ISM) bands.

- **900 MHz:** This range (902 to 928 MHz) supports devices such as wireless headphones and cordless phones.
- **2.4 GHz:** This range (2.400 to 2.4835) supports lower-speed, short-range Bluetooth as well as wireless LAN technologies that conform with IEEE 802.11 standards. Bluetooth is considered a better solution for short-range communication than IR because multiple devices can connect to one device.
- **5 GHz:** This range (5.725 to 5.850) supports IEEE 802.11 standards at a higher power level, providing a wider range and potentially increased speeds.

7.1.2: Wireless technology provides the benefits of increased mobility and a simple method to expand a network beyond the limitations of cables. However, wireless LANs all use the same unlicensed region of the RF spectrum, and multiple devices can interfere with each other. In addition, wireless LANs are more difficult to secure, because unauthorized users within range can intercept (and possibly decrypt) the communication.

7.1.3: The following three categories define common wireless networks:

- **Wireless personal-area network (WPAN):** These networks include PDAs, mice, keyboards, and other short-range IR or Bluetooth devices. WPANs typically are peer-to-peer networks.
- **Wireless local-area network (WLAN):** Typically the wireless portion of a LAN that uses RF technology and IEEE 802.11 standards. An access point (AP) usually provides connectivity for the wireless clients to the wired Ethernet network.
- **Wireless wide-area network (WWAN):** Networks that can use cell phone technologies such as Global System for Mobile Communication (GSM) or Code Division Multiple Access (CDMA) to cover large geographic areas.

7.2.1: An organization called the Wireless Fidelity (Wi-Fi) Alliance tests wireless devices from different manufacturers and ensures that each device meets standards and will function with devices using the same standards. The IEEE 802.11 standard governs implementations of WLANs. Table 7-1 describes the various IEEE 802.11 WLAN standards available.

Table 7-1 IEEE 802.11 WLAN Standards

Standard	Description
802.11	This original standard was released in 1997 and supports a 2-Mbps data rate over the 2.4-GHz frequency. A maximum range is undefined.
802.11a	This amendment was released in 1999 and supports a 54-Mbps data rate over the 5-GHz frequency. The maximum range is estimated to be about 50 meters.
802.11b	This amendment was released in 1999 and supports an 11-Mbps data rate over the 2.4-GHz frequency. The maximum range is estimated to be about 100 meters.
802.11g	This amendment was released in 2003 and supports a 54-Mbps data rate over the 2.4-GHz frequency. The maximum range is estimated to be about 100 meters. 802.11g is backward-compatible with 802.11b.
802.11n	This amendment, released in 2007, supports a 540-Mbps data rate over the 2.4-GHz and 5-GHz frequencies. The maximum range is estimated to be about 250 meters. 802.11n should be backward-compatible with 802.11a, 802.11b, and 802.11g.

Identify and Describe the Purposes of the Components of a Small Wireless Network (Including SSID, BSS, ESS)

Each wireless network is made up of similar components and configurations. Chapter 7 of *CCNA Discovery 1* describes the method of media access, general components, and network grouping available for a WLAN.

CCNA Discovery 1, Chapter 7

7.2.2: A wireless network consists of the following components:

- **Wireless client:** Also called a wireless station (STA). STAs are devices that participate in a wireless network, such as a laptop, printer, server, or PDA.
- **Wireless access point (AP):** Provides connectivity between a wired and wireless network by converting Ethernet frames into 802.11-compliant frames or vice versa. APs support connectivity in a basic service set (BSS) or limited area.
- **Wireless bridge:** Provides connectivity between two wired networks with a wireless link. The link typically is a long-range point-to-point connection over RF frequencies.
- **Wireless antenna:** Can be a directional antenna that concentrates the signal in one direction or an omnidirectional antenna that increases the signal in all directions. Antennas increase signal strength, or gain, and can increase transmission distances.

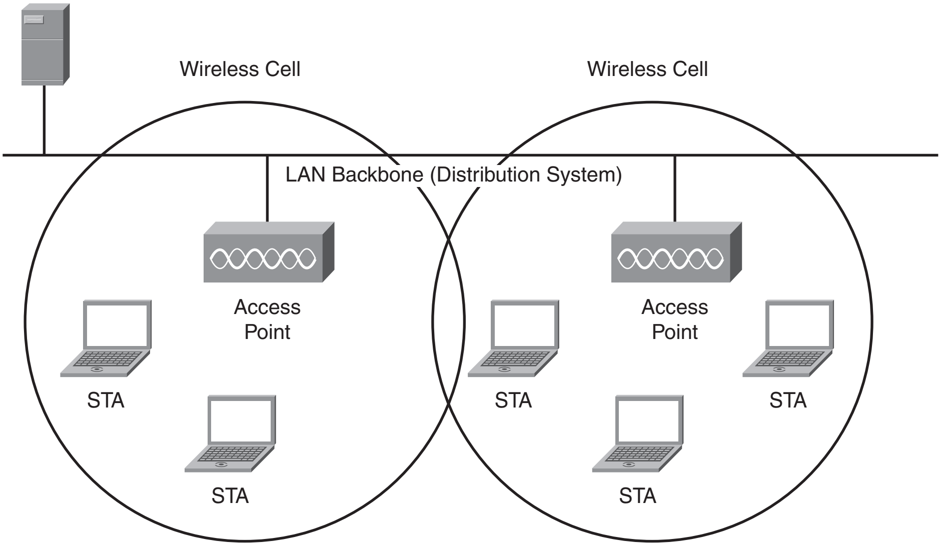
7.2.3: STAs locate a WLAN with a Service Set Identifier (SSID). An SSID is a 32-character, case-sensitive, alphanumeric string located in the header of WLAN frames. Only devices on a WLAN with the same SSID can communicate with each other. In addition, WLANs can be set up in ad-hoc or infrastructure mode. Table 7-2 describes the two basic forms of WLAN installations.

Table 7-2 WLAN Installation Modes

Mode	Network Area	Description
Ad-hoc	Independent basic service set (IBSS) in which devices communicate with each other and are not part of a network.	Simple peer-to-peer direct connection among clients to exchange files and data without an access point.
Infrastructure	BSS in which a group of devices are connected to an AP.	Devices cannot communicate directly; connectivity is centralized, controlled, and directed by an access point.

Multiple BSS access points can be connected by a distribution system (DS) to form an extended service set (ESS). To create an ESS, each BSS access point's range must overlap by 10 percent; this allows a client to move through the ESS without a loss of signal. Figure 7-1 displays an ESS containing two BSS access points connected by a DS.

Figure 7-1 ESS Topology



7.2.4: When you set up an ESS or install a wireless network that has multiple access points (or BSS networks), it is important to use different channels for efficient communication. Multiple access points can overlap in range and divide the available RF spectrum by using separate channels. The wireless standard you choose to implement may have certain channels that overlap or use multiple channels as one channel to increase throughput. Some access points can also automatically choose a channel based on available throughput. If you manually set channels on your installation, look for the channel that will encounter the least interference from other nearby access points.

Wireless networks use an access method called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The following key points define the CSMA/CA process and how a client can reserve a channel:

- A device on a BSS asks permission from the AP to communicate in the form of a request to send (RTS).
- If the channel is available, the AP responds with a clear to send (CTS) message.
- The CTS is broadcast to all devices on the BSS so that all devices know that the channel is in use or that a reservation is in place on the channel.
- When the communication is complete, the sending device sends an acknowledgment (ACK) to the AP, saying that the channel can be released. This ACK is also broadcast to all devices on the BSS to indicate that the channel is available.

Identify the Basic Parameters to Configure on a Wireless Network to Ensure That Devices Connect to the Correct Access Point

Each vendor has creatively customized the configuration tools available for its AP and wireless clients. However, all wireless devices require you to configure the same generic parameters to connect. Chapter 7 of *CCNA Discovery 1* outlines the basic parameters you need to configure to get your WLAN devices talking.

CCNA Discovery 1, Chapter 7

7.2.5: You can use the LAN switch ports on an AP to connect a PC directly to the AP and receive an address through DHCP. Use the **ipconfig** command to determine which gateway is assigned to the computer. Typically you can visit the gateway address in a browser on the connected PC to access the configuration GUI for an AP. Check the documentation with your AP to determine the specific steps to access the configuration. The following common parameters must be configured on a wireless access point to provide connectivity:

- **Wireless or network mode:** This parameter identifies the 802.11 standard supported by the AP, including 802.11b, 802.11a, 802.11g, and 802.11n. An AP can also include a mixed-mode setting to support multiple standards at the same time. Mixed-mode settings can add overhead to the processor and affect network performance.

- **Service Set Identifier (SSID) or network name:** This parameter identifies the WLAN. Any device you connect to the WLAN must have the same SSID. There may also be an option to disable broadcast of the SSID. If SSID broadcast is disabled, you need to add the SSID manually to each client.
- **Wireless channel:** You can manually configure a channel that does not overlap with nearby BSSs, or you can allow the AP to automatically find the best channel.

7.2.6: The following common tools and available parameters allow you to configure a wireless client to connect to a network:

- **Integrated operating system (OS) wireless configuration:** Operating systems such as Windows XP have wireless client software that can provide basic management for a wireless client connection. You cannot use the OS wireless software to manage a connection if you are running a standalone wireless management utility.
- **Standalone wireless utility software:** A wireless network interface card (NIC) often comes with standalone wireless management software. This software can include additional features that display signal strength information, allow for different network profiles, and survey for nearby wireless networks. Standalone software often asks you to disable any operating system wireless management software.
- **Parameters:** To connect to an AP, the client software must share the same SSID as the AP. Typically the wireless utility software detects available networks (with a network survey), and you can select a wireless network. The client then obtains its configuration automatically.

After you have attempted to connect to an access point, you can follow these steps on a client to verify and troubleshoot your wireless connection:

Step 1 Make sure that all devices on your network, including the AP, are powered on, and check LED connectivity indicators for any outside (WAN) connections.

Step 2 Use **ipconfig** to verify that your client computer obtained an IP address and gateway. If you did not receive addressing information, attempt to repair or re-enable the connection.

Step 3 If you receive an IP address, use ping to test connectivity with a remote destination.

Step 4 If you cannot ping outside your network, attempt to ping the AP. If you can successfully ping the AP, check the connection between the AP and outside networks. Use a browser to view the configuration on the AP and verify connectivity with remote networks.

Summary

First you choose a compatible standard to use on your WLAN, and then you select the proper components and design your network. Last, you open the creatively designed graphical interfaces on your wireless devices to configure basic parameters. The convenience of connection provided by a WLAN creates additional concerns about security. We will cover WLAN security on Day 6.

Your Notes

Compare and Contrast Wireless Security Features and Capabilities of WPA Security (Including Open, WEP, WPA1/2)

An unsecured wireless network provides easy access for all users in range, including unauthorized, unwelcome, and possibly evil users. Wireless security features can help you keep the evil out of your network. Chapter 7 of *CCNA Discovery 1* and Chapter 8 of *CCNA Discovery 2* discuss methods available to better secure a WLAN.

CCNA Discovery 1, Chapter 7

7.3.1 and 7.3.2: Unauthorized users attempt to tap into a wireless LAN to obtain free Internet service and possibly steal data from the WLAN. Often an AP signal reaches outside a building or the desired range of the administrator. To avoid malicious war drivers or war walkers, an administrator should implement the following security features on a WLAN during initial setup:

- **SSID broadcast:** You can disable the SSID broadcast feature and require anyone connecting to the network to know the broadcast SSID. However, the SSID is transmitted in clear text, so it is not difficult to discover the SSID for a network.
- **Default settings:** You can change the default settings on your AP, including usernames, passwords, IP addresses, and the SSID to make it more difficult for an intruder to discover the unique settings.
- **MAC address filtering:** You can enable MAC address filtering and specify a list of MAC addresses for devices that are allowed to connect to the network. This requires the manual entry of each MAC address into the list. An intruder can sniff and clone an existing authorized MAC address.

7.3.3: In addition to the default settings and MAC filtering, you can implement authentication for the wireless LAN. Authentication requires the AP to verify a host before it connects to the network using criteria such as a username or password. Authentication occurs before MAC filtering. There are three types of wireless authentication:

- **Open authentication:** Typically used on a public network, open authentication allows all clients to connect to the WLAN. Open authentication is also used in configurations that require separate authentication for the Internet or additional network access as soon as the device has connected to the WLAN.
- **Preshared keys (PSK):** Both AP and client are configured with the same key. When the client requests a connection, the AP asks the client to use the client's key to encrypt a string of information. If the AP can then use its key to decrypt the information, the client is granted access. This is considered one-way authentication because the AP does not authenticate with the host. The user does not have to authenticate, only the host.

- **Extensible Authentication Protocol (EAP):** The EAP software installed on the client communicates with an authentication server such as a Remote Authentication Dial-In User Service (RADIUS). The RADIUS server maintains a database of users separate from the AP. When the user enters a login and password for the network, the AP forwards the login information to the RADIUS server to check its database for validity.

7.3.4: An unauthorized user who cannot authenticate to a network can still intercept wireless frames from a wireless network. You can encrypt all transmission on your network to make it more difficult for an unauthorized user to retrieve data from intercepted frames. Table 6-1 describes two methods of WLAN encryption that allow you to better protect your data.

Table 6-1 WLAN Encryption Protocols

Protocol	Key Length	Description
Wired Equivalent Privacy (WEP)	64 to 256 bits	All devices including the AP must have the same manually configured static key to understand transmissions on the WLAN. Some devices have a passphrase option to make the key easier to remember. Hacking software exists that can extract the static WEP key, so using WEP alone to secure a network is strongly discouraged today.
Wi-Fi Protected Access (WPA)	64 to 256 bits	WPA dynamically generates a different key with each client communication with the AP. The dynamic key makes WPA more difficult to crack than WEP.

7.3.5: In addition to authentication, MAC filtering, and transmission encryption, you can filter network traffic at the AP. The graphical user interface (GUI) in an AP typically allows you to filter network traffic by source and destination MAC address, source and destination port address, and source and destination IP address.

CCNA Discovery 2, Chapter 8

8.2.4: As a quick review with some additional information, remember the following key points about securing a wireless network:

- It is important to change the default settings, such as the SSID and the login, to unique settings for your WLAN.
- You can filter network access by MAC address, but users can clone an authorized MAC address to access the network.
- WEP provides encrypted transmission with a key up to 256 bits. However, WPA provides more secure encryption because it uses temporal key integrity protocol (TKIP) to generate new keys for clients and rotate key use at a configurable interval. WPA also does not require transmission of the key, because both client and AP have the key. WPA2 (802.11i) is an improved version of WPA that uses Advanced Encryption Standard (AES) technology.
- The 802.1x standard can also be implemented on an AP to provide additional security with EAP.

Identify Common Issues with Implementing Wireless Networks

Wireless networks can sometimes suffer from mysterious connectivity issues. The invisible interference and limitations you may encounter while implementing a wireless network are discussed in Chapters 7 and 9 of *CCNA Discovery 1*.

CCNA Discovery 1, Chapter 7

7.4.1–7.4.3: When planning a WLAN, consider the following factors:

- **Coverage areas:** 802.11b/g/n have a larger coverage area than 802.11a.
- **Existing implementations:** 802.11n generally is backward-compatible with 802.11a/b/g, but some access points (AP) do not support the 5-GHz frequency and are not backward-compatible with 802.11a. A preexisting 802.11a installation may require all new equipment to support the same standard if your new APs do not support the 5-GHz frequency.
- **Bandwidth requirements:** All users share bandwidth on a BSS. The number of simultaneous users and type of applications in use can dictate the need for higher-speed equipment.
- **Cost:** Consider the total cost of ownership (TCO), including the equipment, installation, and support.
- **Site survey:** It is important to measure signal strength and interference around the building to determine the most efficient place to install the APs on site.
- **Security:** As mentioned, it is important to plan how you will secure a network. This includes disabling the broadcast SSID, enabling MAC filtering and authentication, setting up WEP or WPA encryption, and filtering unwanted network traffic.
- **Backups:** APs typically have a menu option to back up a configuration to a place you specify on a PC or the network. This allows you to restore the configuration if you forget the password and have to press the reset button to restore your AP to factory defaults. I do this at home about once every four months.

CCNA Discovery 1, Chapter 9

9.3.4 and 9.3.5: Connectivity problems on a WLAN can occur because of authentication issues, interference, signal strength, standards mismatches, and bandwidth issues. Consider the following points when troubleshooting a WLAN:

- **Standards:** The client or AP may be using incompatible standards such as 802.11a on the 5-GHz frequency and 802.11b on the 2.4-GHz frequency.
- **Channels:** Overlapping channels for conversations between devices may be affecting connectivity.

- **Signal:** A lower-strength signal may cause a connection to periodically drop and/or become unreliable. In addition, outside sources such as wireless devices not associated with the WLAN may be interfering with the signal.
- **Bandwidth:** An increase in users or high bandwidth utilization may affect network performance. You can monitor traffic and identify users or applications that hog bandwidth and deal with them professionally, personally, and possibly technically.
- **Association:** Make sure that the case-sensitive SSID is correct on clients and the AP and that a client is not connecting to a different BSS.
- **Authentication:** Check that the same keys, encryption protocols, and proper usernames and passwords are in use on the network.

Summary

Security and a reliable connection are important features in any WLAN. Today you reviewed simple security steps such as SSID configuration and encryption. In addition, you reviewed possible issues that can arise during WLAN implementation, such as channel overlap and signal strength. Day 7 and today provide you with the basic knowledge you need to design, configure, secure, and troubleshoot a WLAN.

Your Notes

Part VI

Days 5–4: Identify security threats to a network and describe general methods to mitigate those threats

Day 5 covers security threats

Day 4 covers security applications

Day 5

Explain Today's Increasing Network Security Threats and the Need to Implement a Comprehensive Security Policy to Mitigate the Threats

The web of security you implement on your network protects your users as well as the time you've invested in implementing a functioning network. The increasing demands placed on networks for speed and reliability require heightened security. Chapter 8 of *CCNA Discovery 1* and Chapter 8 of *CCNA Discovery 2* describe possible threats a network faces and possible policies to protect a network from these threats.

CCNA Discovery 1, Chapter 8

8.1.1: An insecure network is vulnerable to information theft, identity theft, data loss or manipulation, and a possible disruption of service. A network faces external threats from unauthorized users who may attack from the Internet, wireless links, or dialup networks. In addition, internal users with physical and authorized access can intentionally or unintentionally harm a network.

8.1.3: An unauthorized user may employ techniques that trick authorized users into revealing sensitive information or taking an action that threatens a network. The following points describe common social engineering techniques that focus on the user as the weak link:

- **Pretexting:** An attacker contacts a user masquerading as the help desk or creates a scenario convincing the user to reveal sensitive network information. Attackers can research a user to find out information in advance, such as a social security number, to establish legitimacy.
- **Phishing:** An attacker sends an e-mail posing as a legitimate organization and requests verification of account usernames and passwords. Often the e-mail threatens account closure or expiration to entice the user to enter the information.
- **Vishing/phone phishing:** Attackers use Voice over IP (VoIP) to leave a message with a user that claims to be from a banking service. If an unsuspecting user calls the number provided in the message, the user is asked to verify banking information and provide PINs or passwords.

8.2.1: Attackers can also use software in one of the following three forms to gain access to data on a network:

- **Virus:** A program that typically is attached to and activated within another legitimate program that then copies itself and uses system and network resources. Viruses can also damage files and spread through e-mail attachments, downloaded files, and network, CD, or USB device file exchange between computers.

- **Worm:** A program that runs independently and uses a network to send copies of itself to all attached hosts. A self-spreading worm can infect large networks and eventually large parts of the Internet quickly.
- **Trojan horse:** A program that looks like a legitimate program to trick the user into installing the software. Trojans can manipulate files on a computer and provide backdoor access to a computer for remote attacks.

8.2.2: Attackers also use bandwidth and available connections to affect the operation of a network. A denial of service (DoS) attack floods a network or server with traffic, preventing any legitimate connections or use. Table 5-1 describes the various DoS and brute-force attacks.

Table 5-1 Network Service Attacks

Name	Type	Description
Synchronous (SYN) flooding	DoS	Attackers can flood a server with requests from a fake IP address and cause the server to use resources responding to these requests.
Ping of death	DoS	An attacker sends a ping greater than the maximum allowed and causes a system to shut down.
Distributed Denial of Service (DDoS)	DoS	Attackers use multiple hosts to attack a single server or service. Often unsuspecting hosts infected with malicious code are used as robot networks (botnets) to attack a target site.
Brute force	Brute force	Repeated attempts to “crack” a username and password with software that uses any possible combinations.

8.2.3: Spyware and cookies can also pose threats to a computer. Spyware often installs with other programs or web downloads and reports information from your PC to advertisers or other servers on the Internet. Cookies provide a legitimate means for a web server to track information about visitors, but they can be used maliciously to gain information about a host’s web activity.

8.2.4: Unsolicited e-mail advertisements, also known as spam, can overload networks, servers, and hosts with unwanted data and sometimes malicious software. Many network intruders intend to use a compromised system as an e-mail server to send spam over the Internet.

CCNA Discovery 2, Chapter 8

8.1.1: An ISP should secure any web hosting or e-mail services it provides. In addition, an ISP should be the first line of defense for customer security. ISPs can also provide the following security services to customers:

- Help clients create secure passwords and restrictions for devices and software so that only authorized users have access.

- Help clients patch and upgrade software to maintain security, remove unnecessary software applications, and perform security scans on software for vulnerabilities.
- Configure software and hardware firewalls and virus-checking software.

8.1.3: ISPs can also provide data encryption to protect data transmission in the following situations:

- Web servers that provide secure hypertext transfer protocol (HTTPS) instead of clear-text transmission using HTTP.
- Secure e-mail using POP3 and Secure Socket Layer (SSL). An ISP can also provide security for SMTP and IMAP using SSL or Transport Layer Security (TLS).
- SSH instead of Telnet to configure routers or access the command prompt of a server. Telnet transmits in clear text, but SSH is encrypted.
- Secure FTP (SFTP) rather than clear-text FTP.
- IP Security (IPsec) for network layer security to protect any application layer protocols used over a network.

Explain General Methods to Mitigate Common Security Threats to Network Devices, Hosts, and Applications

As the complexity of network attacks increases, so do the defenses against these attacks. Chapter 8 of *CCNA Discovery 1* presents a general overview of the methods available to protect a network.

CCNA Discovery 1, Chapter 8

8.3.1 and 8.3.2: Table 5-2 identifies common methods to mitigate security threats.

Table 5-2 Network Protection Options

Method	Installation	Description
Patch	Periodic software updates	Code released after the original release of the software that fixes an issue with the software.
Update	Periodic software updates	Code released after the original release of the software that can patch issues and add functionality to the software. Many operating systems and applications provide configuration options for automatic updates.
Virus protection	Software on workstation or server	Detects and removes viruses, worms, and Trojan horses.

continues

Table 5-2 Network Protection Options *continued*

Method	Installation	Description
Spyware protection	Software on workstation or server	Detects and removes spyware and adware.
Spam blocker	Software on workstation or server	Detects and removes undesirable e-mails.
Popup blocker	Software on workstation	Prevents a web page from loading additional windows.
Firewall	Hardware device or software on workstation or server	Filters outgoing and incoming network traffic.

Summary

Updates, patches, and virus software maintenance should be routine for any network maintenance plan. In addition, hardware and software firewalls can provide an excellent first line of defense from common outside attacks.

Your Notes

Describe the Functions of Common Security Appliances and Applications

Today you review the protective capabilities of software and firewalls for a network. Chapter 8 of *CCNA Discovery 1* and Chapter 8 of *CCNA Discovery 2* outline the functions of antivirus software and firewalls as well as the sensors available to prevent network intrusions.

CCNA Discovery 1, Chapter 8

8.3.3: Antivirus software can prevent initial infection and sometimes remove infected files and repair an infected system. Antivirus software can scan files and programs as they open, scan e-mails as they arrive on the system, update automatically, and run full scheduled scans of a system. It is important to update antivirus software, because new virus patterns continually surface on computers and the Internet.

8.3.4: Antispam software attempts to filter any unwanted, unsolicited e-mails from your system. Spam filters can be loaded on individual workstations or on an e-mail server. Some spam e-mails contain false warnings about your system and advise you to install software or make system configuration changes. It is important to check that any warning e-mail is not a hoax before acting.

8.3.5: Antispyware software can detect and remove spyware/adware or cookies and prevent future installs of adware or spyware. Spyware collects information about a system and often configures the system to reinstall the spyware if it is removed. Spyware can slow system performance and render a system vulnerable to other attacks. Similarly, popups on websites can attempt to install spyware or simply annoy the user. Most web browsers come with a popup blocker that you can configure to allow necessary popups and block unnecessary ones.

8.4.1: Firewalls are installed between two networks and can control traffic in the following ways:

- Filter traffic based on destination and source IP address or MAC address.
- Block websites based on uniform resource locator (URL) or keywords.
- Filter traffic based on the type of application used for network transmission.
- Inspect incoming traffic, and ensure that each incoming packet is a response to a legitimate outgoing request. This stateful packet inspection (SPI) can prevent DoS attacks.
- Firewalls can also provide network address translation (NAT) for additional security on an internal network.
- A firewall can come packaged as a standalone security appliance, a server-based firewall that installs on a network operating system (NOS), a module that can be installed or is integrated inside an existing router, or a personal firewall that installs on a network host.

8.4.2: A firewall can protect users on the intranet from Internet attacks; however, some network devices may need greater access to and from the outside world. For example, a web server could be placed outside the internal network, yet still receive some protection from a separate firewall protecting similar, less secure devices. Servers outside the internal network protected by another firewall are in the demilitarized zone (DMZ). The DMZ typically is an area more secure than a direct connection to the Internet located between an internal and external firewall. On the other hand, when setting up a smaller network, you can create a subnet and configure a single integrated router/firewall to provide DMZ levels of security to only specific devices such as a web server. A standard DMZ allows incoming requests on standard server ports such as 80 (HTTP), 21 (FTP), and 110 (POP3) .

CCNA Discovery 2, Chapter 8

8.2.2: The Cisco IOS Firewall software is included with the Cisco IOS. It allows you to control traffic between networks with access lists. In addition, routers can filter packets dynamically and monitor communication with a state table. A stateful firewall uses this dynamic monitoring to guarantee that all traffic belongs to legitimate communications.

On larger networks you usually design firewall security in layers. Border routers filter packets and route traffic to the DMZ or an internal firewall. The internal firewall only allows outside traffic that was specifically requested by an internal device. Additional internal firewalls may separate and protect sensitive areas such as network devices containing financial and personal data. These additional firewalls can provide an extra layer of security in case an internal host is infected with a Trojan horse, worm, or virus.

8.2.3: Table 4-1 describes two types of sensors available to detect and prevent network intrusions.

Table 4-1 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

System	Implementations	Description
IDS	Software (Cisco IOS IPS), hardware, Adaptive Security Appliance (ASA)	Monitors traffic (on one port) and notifies a management station. Can detect only the first malicious transmission, but can reconfigure the router to block future attacks. Used on the network perimeter in front of a firewall to analyze attacks or behind a firewall to detect firewall configuration issues.
IPS	Software (Cisco IOS IPS), hardware, ASA	Traffic passes through the IPS (in one port and out another), which filters suspicious traffic in real time. Can examine the entire data packet from Layer 7 to Layer 2. Usually placed behind a firewall to further examine packets destined for the internal network.

Describe Security Recommended Practices, Including Initial Steps to Secure Network Devices

A paranoid network administrator is a good network administrator when it comes to protecting network devices and hosts. Chapter 8 of *CCNA Discovery 1* and Chapter 8 of *CCNA Discovery 2* outline available software and steps to monitor and protect network devices and network activity.

CCNA Discovery 1, Chapter 8

8.4.3: Software tools such as the Microsoft Baseline Security Analyzer (MBSA) allow you to scan your network for vulnerable areas and determine possible weak points for attacks. When considering network vulnerability, you could document the number of hosts, the services that each host offers, the operating systems of the hosts, and any packet filters or firewalls in use on the network.

CCNA Discovery 2, Chapter 8

8.1.2: To protect data on a server, an administrator can encrypt the data and grant differing levels of access based on user accounts and group membership. Also, an administrator can use the following three-step process of authentication, authorization, and accounting (AAA) to improve security:

Step 1 **Authentication** requires users to verify their identity with a username and password using a RADIUS or TACACS server.

Step 2 **Authorization** limits access for users based on rights assigned to the user account by the administrator.

Step 3 **Accounting** tracks user network activity and application use.

Summary

Security should be a consideration in every step of the network design, implementation, and maintenance process. Antivirus software, firewalls, IPS, IDS, and the AAA process provide you with the tools and steps you need to properly design and protect a network.

Your Notes

Part VII

Days 3–1: Implement and verify WAN links and review all days

Day 3 covers WAN connections

Day 2 covers Packet Tracer skills review

Day 1 covers a final overview

Describe Different Methods of Connecting to a WAN

After the LAN has been planned, put together, and secured, you can connect to the outside world or other LANs with a WAN connection. Chapter 5 of *CCNA Discovery 2* identifies available WAN connections.

CCNA Discovery 2, Chapter 5

5.5.3 and 5.5.4: Table 3-1 describes the WAN connections a telecommunications service provider (TSP) can offer individuals and organizations.

Table 3-1 WAN Connection Types

Connection Type	Description	Example
Point-to-Point Protocol (PPP)	A specific dedicated path through the TSP network that connects two LANs over a large geographic area.	An ISP typically provides leased lines to facilitate a PPP connection.
Circuit-switched	Allows the client to create and close connections over the TSP network. This connection operates like a phone call.	Integrated Services Digital Network (ISDN) or dialup network access.
Packet-switched	A client uses a software-managed virtual circuit over a shared connection.	Frame Relay.

In addition to the type of connection, consider the following points about specific WAN connections when planning a network:

- Lower-speed, low-cost connections such as dialup and beginning plans for Frame Relay and DSL provide sufficient connectivity for a business that does not host services and that needs only occasional connectivity with smaller downloads.
- Medium- to high-speed connections such as a fractional or full T1 or advanced DSL and Frame Relay plans can provide connectivity for a medium-sized business that plans to host minimal services and occasionally download large amounts of data. In addition, a cable network connection can provide a high-bandwidth solution.
- A business planning to host major online servers and that requires a reliable high-bandwidth connection should consider WAN connections that include a service level agreement (SLA) and possibly a very high-bandwidth connection, such as a T3, SONET, or ATM.

Configure and Verify a Basic WAN Serial Connection

Routers sometimes use a serial interface to connect to a WAN device provided by an ISP. Chapter 5 of *CCNA Discovery 2* outlines the protocols, devices, and configuration steps to set up a basic WAN serial connection.

CCNA Discovery 2, Chapter 5

5.2.3 and 5.5.6: After you have connected your router or customer premises equipment (CPE) device to the Channel Service Unit/Data Service Unit (CSU/DSU) provided by the ISP, you need to configure the interface on the router. If the interface is a serial interface, the CSU/DSU provides the clock rate as the data circuit-terminating equipment (DCE), and your router acts as the data terminal equipment (DTE).

The Cisco default encapsulation for a serial interface is High-Level Data Link Control (HDLC); however, you can change the encapsulation to PPP as a more flexible, nonproprietary encapsulation. In addition, PPP supports authentication in clear-text Password Authentication Protocol (PAP) or encrypted Challenge Handshake Authentication Protocol (CHAP). A router can also use Frame Relay as an encapsulation. Frame Relay virtual circuits use HDLC encapsulation, and each circuit is identified by a data link connection identifier (DLCI).

You can select one of the following address types for a serial WAN connection:

- **A static IP address** allows the administrator to manually enter the IP address and subnet mask. This option is available for PPP, Frame Relay, and HDLC.
- **IP unnumbered** sets the interface to match the IP address of another enabled interface on the router. This option is available for PPP, Frame Relay, and HDLC.
- **IP negotiated** is available for PPP and allows the router to obtain address information automatically from the ISP.

You can set the encapsulation and address type in the graphical Cisco SDM, or you can use the **encapsulation** command in interface configuration mode at the command-line interface. To verify addressing and encapsulation for an interface, use the **show interface** command.

5.3.5: Example 3-1 demonstrates the configuration commands for a basic DTE serial connection to a WAN using PPP encapsulation.

Example 3-1 Router DTE Serial Interface Configuration Using PPP

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# interface serial 0/0
RouterA(config-if)# description Connection to WAN
RouterA(config-if)# ip address 192.168.2.5 255.255.255.252
RouterA(config-if)# encapsulation ppp
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# exit
RouterA# copy running-config startup-config
```

The following commands allow you to verify your interface configuration:

```
show running-config
show interfaces
```

Summary

It is important to consider factors such as bandwidth, connectivity needs, and cost when choosing a WAN connection. Often the options depend on the WAN provider. A quick review of today provides basic information about WAN connection types and how to configure a WAN serial connection to your router.

Your Notes

Day 2

CCNA Discovery 1 Packet Tracer Activity Checklist

These Packet Tracer activities located in the *CCNA Discovery 1* online curriculum suggest skills and concepts you should review before the CCENT/ICND1 exam. Skim through the following activities and practice them, and then check off each activity you can comfortably complete. You can revisit each activity in the curriculum using the section number next to each checkbox.

- ❑ **3.5.7.2:** Become familiar with the Packet Tracer user interface. Model a simple network, and observe network behavior. Create an Ethernet network using two hosts and a hub, and observe ARP, broadcast, and ping (ICMP) traffic.
- ❑ **3.6.2.3:** Prototype a simple network consisting of two hosts and a switch.
- ❑ **4.2.3.2:** Use ping and traceroute to check connectivity and learn more about how packets travel through the Internet.
- ❑ **5.1.1.2:** Use Packet Tracer to ping different websites.
- ❑ **5.3.3.3:** Configure a device as a DHCP server, and specify a range of IP addresses. Configure a DHCP client, and verify the DHCP configurations.
- ❑ **5.4.3.2:** Configure a multifunction device as a DHCP server, and configure a client to receive the IP configuration. Verify the configuration of public and private addresses.
- ❑ **6.2.2.2:** Observe traffic requests when a client browser requests web pages from a server.
- ❑ **6.3.3.5:** Use Packet Tracer to view PDU information being sent between a client and server.
- ❑ **9.2.3.2:** Use the **ipconfig** command to examine IP configuration information on a host.
- ❑ **9.2.4.3:** Use ping to examine end-to-end connectivity between hosts.
- ❑ **9.3.5.2:** Given a scenario, determine why a wireless STA is unable to connect to a WLAN, and correct the problem.

CCNA Discovery 2 Packet Tracer Activity Checklist

These Packet Tracer activities located in the *CCNA Discovery 2* online curriculum suggest skills and concepts you should review before the CCENT/ICND1 exam. Skim through the following activities and practice them, and then check off each activity you can comfortably complete. You can revisit each activity in the curriculum using the section number next to each checkbox.

- ❑ **2.3.1.3:** Troubleshoot and resolve a network connectivity issue.
- ❑ **3.1.3.2:** Create a logical and physical network diagram.

- ❑ **3.3.3.4:** Explore different LAN switch options.
- ❑ **3.3.4.3:** Explore different internetworking device options.
- ❑ **4.1.5.2:** Modify the addresses, subnet masks, and device default gateways to enable routing between subnets.
- ❑ **5.1.5.2:** Explore the running and startup configuration of a router using the Cisco IOS CLI.
- ❑ **5.3.2.5:** Log into a router, and practice using the help functions to navigate through different modes.
- ❑ **5.3.3.3:** Explore the **show** commands to reveal the configuration details of routers in a network.
- ❑ **5.3.4.4:** Use Packet Tracer to perform an initial router configuration.
- ❑ **5.3.5.4:** Use Packet Tracer to configure an Ethernet interface and a serial interface.
- ❑ **5.3.6.2:** Use Packet Tracer to configure a default route on routers in a medium-sized business network topology.
- ❑ **5.3.7.2:** Use Packet Tracer and the Cisco IOS CLI to configure a router as a DHCP server for attached clients.
- ❑ **5.3.8.2:** Use Packet Tracer and the Cisco IOS CLI to configure static NAT on a router.
- ❑ **5.3.9.2:** Use Packet Tracer to copy a router's running configuration to the start-up configuration, and then back up the running configuration to a TFTP server.
- ❑ **5.4.3.4:** Perform a basic switch configuration.
- ❑ **5.4.4.2:** Configure and connect the switch to the LAN using a configuration checklist.
- ❑ **5.4.4.5:** Use the CDP **show** commands to discover information about devices in the network.
- ❑ **5.5.6.2:** Use Packet Tracer to configure a serial WAN connection from a Cisco ISR to a CSU/DSU at an ISP.
- ❑ **6.1.1.5:** Manually configure and reconfigure static routes.
- ❑ **6.1.5.3:** Configure and verify RIP.
- ❑ **8.2.2.3:** Position firewalls on a network diagram for a medium-sized business.
- ❑ **8.2.4.2:** Configure WEP security between a computer and a wireless router.
- ❑ **9.0.1.2:** Use the knowledge and skills presented in this course to perform a simulated network upgrade. Create an IP addressing plan for a small network. Implement a network equipment upgrade. Verify device configurations and network connectivity.

Summary

Your comfort with these skills in Packet Tracer will directly affect your attitude and performance on the simulation portion of the CCENT/ICND1 exam. If you are still involved with your Cisco

Networking Academy, you may have your instructor initial each activity you complete successfully; you could even select a few activities and race other academy students. Your instructor will likely not race you for fear of embarrassment.

Your Notes

Day 1

Review Detail Charts, Lists, and Concepts from Previous Days

Day 1 provides the key commands and general concepts you should recognize and be able to expand on during your exam and as a network technician. If any concepts mentioned today seem unfamiliar, be sure to look them up in this book, the curriculum, or on the web. It may also help to further distill the concepts you read today into your own personal outline for your memory in the notes section provided at the end of this day.

Day 31: Network Components and Operation

The following list and Table 1-1 describe network device purposes at each layer of a three-layer hierarchical model:

- **Access layer devices** connect hosts on a local-area network (LAN) to provide access for users.
- **Distribution layer devices** provide connectivity between LANs.
- **Core layer devices** provide high-speed connectivity between distribution layer devices.

Table 1-1 Networking Devices and Their Purposes

Device	Layer	Purpose
Hub	Typically installed in a LAN at the access layer	Ethernet networking device with multiple ports that simply regenerates a signal it receives on one port to all other ports. All devices are on the same channel and share that channel's bandwidth. If two devices send a message at the same time, a collision occurs.
Switch	Used at the access layer	Multiport networking device that looks at the destination physical address of a received frame on one port to forward the frame to the port where the host is connected. Hosts communicate through temporary circuits, avoiding collisions.
Router	Connected at the distribution layer	Routers look at the destination IP address of a received packet and forward the packet to its destination network. Routers also determine the best path for a packet to its destination network.

Day 30: Layered Model Applications

The benefits of a layered model are as follows:

- It helps with the design of protocols, because each layer has a standard function and a standard interface for communication with other layers.
- It allows products from different vendors to work together, allowing for collaboration in design and competition between manufacturers of compatible components.
- It allows the technology of one layer to improve without affecting other layers.
- It provides common terminology to teach, learn, and discuss networks and network protocols.

Table 1-2 compares the OSI seven-layer model and the TCP/IP model.

Table 1-2 OSI Seven-Layer Model and TCP/IP Model

OSI Layer Name	Protocols (Example)	PDU	TCP/IP Layer Name
7 (Application)	E-mail, FTP, and HTTP	Data	Application
6 (Presentation)	ASCII	Data	
5 (Session)	SQL	Data	
4 (Transport)	TCP, UDP (port 80)	Segments	Transport
3 (Network)	IP (192.168.1.1)	Packets	Internet
2 (Data link)	MAC (00-00-0C-1A-22-3B)	Frames	Network access
1 (Physical)	Bits (1010010001010001)	Bits	

Layer 2 of the OSI model, the data link layer, is made up of two layers: the upper logical link control (LLC) layer, and the lower media access control (MAC) layer. The Ethernet protocol operates at the data link layer as well as the physical layer of the OSI model.

Day 29: Layered Model Protocols and Their Purposes

Tables 1-3 through 1-5 describe the standards and protocols implemented in layered models.

Table 1-3 Ethernet Standards

Standard	Description
DIX standard	Digital, Intel, and Xerox standard for 10 Mbps over coaxial cable
IEEE 802.3 10BASE5	10-Mbps baseband over coaxial cable (thicknet) capable of a 500-meter distance
IEEE 802.3a 10BASE2	10-Mbps baseband over coaxial cable (thinnet) capable of a 200-meter distance

Standard	Description
IEEE 802.3i 10BASE-T	10-Mbps baseband over twisted-pair copper capable of a 100-meter distance
IEEE 802.3j 10BASE-F	10-Mbps baseband over fiber
IEEE 802.3u 100BASE-T	100-Mbps baseband over twisted pair
IEEE 802.3z 1000BASE-X	1 gigabit per second (Gbps) baseband over fiber
IEEE 802.3an 10G BASE-T	10 Gbps over twisted pair

Table 1-4 Client/Server Protocols

Type	Protocols/Ports	Description
Web servers	HTTP/80 HTTPS/443	Clients make a request of a server on port 80 using HTTP, and the server responds with a web page created in hypertext markup language (HTML). Secure requests occur using HTTPS.
FTP servers	FTP/21 FTP/20	An FTP client makes a request to a server on port 21. As soon as the session is open, the server responds with data on port 20.
E-mail servers	SMTP/25 POP3/110 IMAP4/143	A server sends and stores e-mails accessed by an e-mail client. Clients and servers use simple mail transfer protocol (SMTP) to send e-mails. Servers use post office protocol (POP) to receive and store messages. Servers can also allow an Internet message access protocol (IMAP) client to receive and store messages and keep the messages in the mailbox on the server.
IM Servers	Various depending on vendor	Users can install compatible IM clients and communicate instantly with other users on the same IM network.

Table 1-5 TCP Versus UDP

TCP	UDP
Connection-oriented protocol	Connectionless protocol
Reliable protocol with acknowledgment, retransmission, flow control, and sequencing	Unreliable; requires reliability to be implemented in other layers if needed
Greater network overhead	Less network overhead
Used for e-mail, FTP, and web applications that require reliable transmission	Used in DNS, SNMP, DHCP, RIP, TFTP, VoIP (some of TCP's reliability is added to VoIP traffic with the use of Real-Time Transfer Protocol), online games, video, and audio

Day 28: Network Diagrams and Components

A physical topology displays actual device and wiring locations to help you efficiently locate and troubleshoot devices. Physical topologies can be categorized as bus, ring, mesh, or star topologies.

A logical map of the network topology groups hosts and devices by how they use the network. A logical topology map displays hostnames, address groups, network access, and applications in use on a network.

Table 1-6 describes the features of hubs and switches.

Table 1-6 Functions of Hubs and Switches

Hubs	Switches
Multiple ports. Regenerates a received signal out all ports except the port where the signal is received.	Multiple ports. Reads each frame's MAC address, maintains a MAC table of which hosts are attached to each port, and forwards frames based on the destination MAC address.
Shared bandwidth. All devices see a transmission from one device, and only one device can communicate at a time.	Hosts connected to a switch do not share bandwidth, because the switch creates temporary circuits between communicating hosts based on MAC addresses.
All connected devices are in the same collision domain, because a collision occurs if any two devices send at the same time.	Multiple conversations can occur without collisions because of the temporary circuits, so each port is its own collision domain on a switch.
If a collision occurs on a hub, the hub still forwards the frame with errors out all ports. The NICs on the hosts discard the frame.	The switch builds its table from source MAC addresses in frames from sending hosts. If the switch does not yet know a frame's destination MAC address, it floods the frame out all other ports. Switches do not forward frames with errors or frames with the same source and destination.

The following key points define routers:

- Routers connect networks and route packets to their destination networks.
- Routers can look at the MAC address to determine a frame's destination, but routers also decapsulate the frame to look at the destination IP address located in the header of the IP packet.
- Routers look at the network portion of the destination IP address, re-encapsulate the packet, and forward it to its destination.
- Routers maintain a routing table of connected networks. When a router receives a packet, it references the routing table to determine which interface connects to the destination network.
- Routers do not forward frames with a broadcast MAC address, so each port on a router is its own broadcast domain. In other words, **routers divide broadcast domains.**

Day 27: Troubleshooting and LAN Versus WAN

The following commands display information about connectivity and configuration on a device. Table 1-7 describes general troubleshooting tasks for each OSI layer.

- **ipconfig** shows the IP configuration.
- **ping** tests network layer connectivity between devices.
- **tracert** tests connectivity and displays each hop.
- **netstat** shows any network connections to the device.
- **nslookup** queries the configured name server for DNS information.

Table 1-7 Troubleshooting for Each OSI Layer

Layer	Areas to Troubleshoot
Physical layer (1)	Power, connectivity, cables, LEDs, temperature, and humidity.
Data link layer (2)	Switch and NIC configurations and operation.
Network layer (3)	IP configurations on devices. Use **ping**, **ipconfig**, and **tracert**.
Transport layer (4)	Firewall and filtered TCP or UDP ports.
Session, presentation, and application layers (5 through 7)	Settings in your applications for encryption, authentication, or additional configuration requirements. Use Telnet or a network traffic analyzing tool.

LANs today often represent the logical grouping of hosts for a single organization. Network administrators typically refer to the network they maintain in their building (or buildings) as a LAN or private intranet. LANs support high data transfer rates over Ethernet or wireless protocols in a smaller geographic area. A WAN provides relatively lower data transfer rates over a larger geographic area.

Day 26: Network Physical Media

Table 1-8 describes networking cables often used in network implementations, such as twisted pair, coaxial cable, and fiber-optic cable.

Table 1-8 Common Network Cables

Cable Name	Description	Types
Twisted pair	Twisted wires that carry electrical signals susceptible to crosstalk and outside electrical interference. The twists in the wire pairs reduce crosstalk.	Category 5 unshielded twisted pair (UTP), Category 3 UTP, Category 6 UTP, and Category 7 screened twisted pair (ScTP). Terminated with an RJ-45 connector.
Coaxial	Carries electrical signals over a copper wire. Shielded and capable of longer lengths than UTP, but more expensive and difficult to install. Used for cable network offerings.	Coaxial cable terminated with a BNC type or F series connector.
Fiber-optic	Two fiber-optic cables to send and receive data with pulses of light. Consists of a coating, cladding, and glass core. Multimode is less expensive than single-mode fiber. Used for long distances and as backbone connections inside or between buildings.	Multimode runs a shorter distance with multiple rays of light from LEDs. 2000-meter limit. Single-mode provides a single path for an LED laser and can run a longer distance (3000 meters).

The following points define the standards for UTP cables:

- TIA/EIA defines the T568A and T568B wiring schemes for network cables. Be sure to use the same scheme for an entire installation project. UTP cables typically are terminated with an RJ-45 jack that plugs into an RJ-45 connector.
- When you design your network, all your cables typically will terminate in a patch panel, and you will use patch cables to connect network devices. You use a punchdown tool to set the wires from a UTP cable properly in a patch panel.
- A straight-through cable is wired with the same scheme on both ends. A crossover cable is wired with T568A on one end and T568B on the other.
- Some devices can sense the pins available and adjust the port to work with either a crossover or straight-through cable. You can test cables with a cable tester, cable certifier, or multimeter.

The following networking cables serve different purposes:

- **A crossover cable** connects similar devices: hub to hub, switch to switch, PC to PC.
- **A straight-through cable** connects devices that are not similar: hub to PC, switch to PC, switch to router.

- **A console cable** connects to the console port on a router or switch to configure the device.
- **A serial cable** is often used to connect a router to an Internet connection.

Day 25: Media Access Control and Segmentation

When Ethernet devices in the same collision domain attempt to communicate at the same time, a collision occurs. Each device detects the collision and waits a random amount of time before attempting to retransmit. Hosts on an Ethernet network use this process to ensure that only one host transmits at a time on a single collision domain; this process is often called **carrier sense multiple access collision detect (CSMA/CD).**

A switch increases the number of collision domains because it filters and forwards frames based on the source and destination MAC. A switch's ability to divide collision domains is often called **microsegmentation** of the network. However, switches still forward all frames with FFFF.FFFF.FFFF as the destination MAC address because it is a broadcast frame. When bandwidth needs or host numbers increase, broadcast traffic begins to slow a network. Routers do not forward broadcast frames; **routers divide broadcast domains.**

Day 24: Switch Operation

Remember the following key points about switch ports:

- A switch port can operate in full-duplex mode, allowing it to send and receive data simultaneously.
- A switch port can also operate in half-duplex mode, allowing the port to alternately send and receive data, but not simultaneously send and receive.
- When a device is connected to a switch, the switch attempts to autonegotiate the speed and either full- or half-duplex transmission. If the other device does not support autonegotiation, the switch defaults to the speed of the other device and half-duplex.
- An administrator can turn off autonegotiation and manually set the switch to full or half duplex. If a connected device is incapable of autonegotiation, you can set the switch to the matching duplex of the device, and the switch adjusts for the speed of the connection.
- Switches can operate in **store and forward mode**, in which the entire frame is received before sending, or **cut-through mode**, in which the switch looks at only the first part of the frame before forwarding.
- Switches use Spanning Tree Protocol (STP) to avoid switching loops and set ports as blocking, listening, learning, or forwarding.

Day 23: Switch Configuration

The Cisco IOS command-line interface (CLI) provides the following levels of access:

- **User access or user EXEC:** Default access. Shows basic information about the operation and connectivity.
- **Privileged EXEC:** Allows you to adjust the operation of a switch and view configuration files.
- **Global configuration:** Allows you to configure the device and enter submodes for specific configurations.

Example 1-1 Initial Configuration on a Switch

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname Switch22
Switch22(config)# line console 0
Switch22(config-line)# password cisco
Switch22(config-line)# login
Switch22(config-line)# line vty 0 4
Switch22(config-line)# password cisco
Switch22(config-line)# login
Switch22(config-line)# exit
Switch22(config)# enable password cisco
Switch22(config)# enable secret class
Switch22(config)# interface vlan 1
Switch22(config-if)# ip address 192.168.1.2 255.255.255.0
Switch22(config-if)# no shutdown
Switch22(config-if)# exit
Switch22(config)# ip default gateway 192.168.1.1
Switch22(config)# exit
```

Day 22: Switch Security

Table 1-9 provides examples of commands available to implement switch security.

Table 1-9 Switch Security Commands

Configuration Commands	Verification Commands
switchport mode access	**show mac-address-table**
switchport port-security	**clear mac-address-table**

Configuration Commands	Verification Commands
switchport port-security mac-address sticky	**show port-security** **show running-config** **show interfaces** **show vlan**

Here's the command syntax to assign a static MAC address:

```
mac-address-table static {host-mac-address} interface {interface} vlan {vlan}
```

Here's the command syntax to set speed and duplex on a switch port:

```
speed {speed-in-megabits-per-second}
duplex {half ¦ full}
```

Day 21: Switch Troubleshooting

Table 1-10 provides examples of commands available to troubleshoot a switch.

Table 1-10 Switch Troubleshooting Commands

show Commands	cdp Commands
show running-config	**show cdp**
show startup-config	**show cdp neighbors**
show version	**show cdp neighbors detail**
show interfaces	
show mac-address-table	
show port-security	

Day 20: IP Addressing

Tables 1-11 through 1-13 describe how networks are divided by class and additionally through subnetting.

Table 1-11 Class A, B, C, D, and E Networks

Class	Binary Start	First Octet Range	Subnet Mask and Number of Network (N) and Host (H) Octets	Hosts	Bits in the Network Address
Class A	0	1–126	255.0.0.0 N.H.H.H	About 16 million	8
Class B	10	128–191	255.255.0.0 N.N.H.H	65,535	16
Class C	110	192–223	255.255.255.0 N.N.N.H	254	24
Class D	111	224–239	H.H.H.H	Multicast	28
Class E	1111	240–255	Research	Research	Research

Table 1-12 RFC 1918 Private Networks and the Loopback

Class	Address Range (Number of Addresses Available)
Class A	10.0.0.0–10.255.255.255 (more than 16 million)
Class B	172.16.0.0–172.31.255.255 (more than 65,000)
Class C	192.168.0.0–192.168.255.255 (254)
Loopback	127.0.0.0–127.255.255.255

Table 1-13 Borrowed Bits to Divide a Default Class C Network

Slash Format	/25	/26	/27	/28	/29	/30	/31	/32
Last Octet in the Mask (in Decimal)	128	192	224	240	248	252	254	255
Bits Borrowed	1	2	3	4	5	6	7	8
Total Subnets	2	4	8	16	32	64	—	—
Total Hosts	128	64	32	16	8	4	—	—
Useable Hosts	126	62	30	14	6	2	—	—

Day 19: Assign Addresses

Static address assignment on a host guarantees that it will always have the same IP address on the network. Hosts that provide services such as servers and printers usually receive static IP addresses. DHCP provides a manageable way to maintain a **dynamic addressing** scheme.

The following general commands allow you to assign an IP address to an interface in Cisco IOS software:

```
enable
configure terminal
interface interface
ip address ip-address subnet-mask
no shutdown
```

Day 18: NAT

The following list defines the various addresses and networks used in NAT. Table 1-14 lists NAT configuration and verification commands.

- **Inside local network:** The privately addressed internal network connected to a router.
- **Inside local address:** A private internal IP address assigned to hosts attached to the inside local network.
- **Outside global network:** Any network outside of the local network that would not recognize the private addresses assigned to hosts in the local network.
- **Inside global address:** An IP address of a host attached to the local internal network as it appears to the outside network—the translated IP address.
- **Outside local address:** The packet's destination address while on the inside local network. Typically the same as the outside global address.
- **Outside global address:** The actual destination address of the intended external host on the Internet.

Table 1-14 NAT Configuration and Verification

Configuration	Verification
ip nat outside	**show running-config**
ip nat inside	**show ip nat translation**
ip nat inside source static *local-IP-address global-IP-address*	**debug ip icmp**
	ping

Day 17: DNS Operation

The following steps occur when a host wants to resolve a DNS name such as mail.cisco.com:

1. The host uses a resolver to query a DNS server inside its domain for the IP address of mail.cisco.com. This DNS server is preconfigured for the host.

2. The DNS server receives the request and checks its local records. If the DNS server cannot resolve the domain name, it forwards the request to another preconfigured DNS server. The local DNS server may query a root DNS server to discover the location of top-level .com domain name servers.

3. The top-level DNS server, after it is queried, responds with the location of the cisco.com DNS server for the requested domain.

4. The local DNS server queries the cisco.com DNS server for the location of mail.cisco.com. When the resolved name to IP address is returned, each DNS server caches the record for a limited amount of time.

The local DNS server receives the returned request, temporarily caches the record, and responds to the requesting host with the IP address for mail.cisco.com.

Day 16: Private Networks and NAT

The following key points summarize the operation and benefits of public and private addressing:

- A device directly connected to the Internet has a public IP address. This address is routable. Other devices on the Internet can identify, locate, and request services from a device with a public IP address.

- The number of public IP addresses is limited, so RFC 1918 reserves Class A, B, and C networks for private use on an internal network. These address ranges can be reused for multiple internal networks because the networks are not visible to the Internet or each other.

- A router running NAT and PAT can allow devices on a private network to share a single public IP address and communicate over the Internet.

- Devices on a private network behind a router running NAT are not directly accessible on the Internet, providing additional security.

Day 15: DHCP Operation

A client that needs an IP address follows these steps to obtain an IP address on a DHCP network:

Step 1 The client sends a DHCP Discover message with a destination IP address of 255.255.255.255 and a destination MAC address of FF-FF-FF-FF-FF-FF.

Step 2 This DHCP Discover message broadcasts over the network, and the DHCP server replies with a DHCP Offer, including a suggested IP address.

Step 3 The requesting client sends a DHCP Request to use the IP address suggested in the DHCP offer.

Step 4 The DHCP server responds with a DHCP Acknowledgment.

Table 1-15 outlines the configuration commands and parameters necessary to implement and verify DHCP.

Table 1-15 DHCP Configuration and Verification

Configuration	Verification
ip dhcp pool *pool-name*	**show running-config**
network *network-address subnet-mask*	**show ip dhcp binding**
domain-name *domain-name*	**show ip dhcp server statistics**
dns-server *dns-server-address*	**debug ip dhcp server events**
default-router *default-router-address*	
lease {*days* [*hours*] [*minutes*] | **infinite**}	
ip dhcp excluded-address *start-address end-address*	
ip dhcp excluded-address *single-address*	

Day 14: Static and Dynamic Addressing

You can assign an address to hosts in your LAN in one of these ways:

- **Manual configuration:** You can enter a static IP address, subnet mask, and gateway on hosts in your network. These static addresses remain the same for these devices unless you manually change them.
- **Dynamic configuration:** You can configure a DHCP server to dynamically assign addresses to computers on your network. You can specify the address range, client lease, and other parameters on the DHCP server. You also need to configure clients to request addressing information from the DHCP server.

Day 13: IP Address Troubleshooting

If your computer is configured to obtain an IP address automatically, you can follow these steps to check DHCP operation:

Step 1 Check the IP configuration on your host. Open a command prompt, and enter the command **ipconfig /all**. Look at the subnet mask, gateway, DNS settings, and IP address.

Step 2 Make sure that the gateway and host IP addresses are on the same network.

Step 3 Try releasing and renewing the dynamic IP address with the commands **ipconfig /release** and **ipconfig /renew**.

A successful ping to your gateway router followed by an unsuccessful ping to an Internet address indicates a problem with your connection between the router and the ISP. You can first check that your router has a public IP address and a proper configuration to communicate with the ISP. You may have to contact the ISP to troubleshoot the connection to its network.

Day 12: Routing and Routers

Protocols such as IP are **routed protocols** because a router uses the protocol to forward a packet from one router to another. In contrast, the **routing protocols** discussed on Day 12 are used by routers to exchange routing information.

Table 1-16 describes the various types of routes you may encounter while reading a routing table. Table 1-17 compares the features of distance vector and link-state routing.

Table 1-16 Routes in the Routing Table

Route Type	Features
Directly connected	The router detects configured networks connected to its interfaces and adds them to the routing table automatically. These routes are identified by the prefix C. They automatically update when the configuration changes or an interface is shut down.
Static	This is a manually configured route added by the administrator. It is identified by the prefix *S*.
Dynamic	Routers use routing protocols to communicate information about routes in their routing table. These routes are dynamically updated by the routing protocol. The prefix for a dynamic route is based on the type of protocol. For example, Routing Information Protocol (RIP) is identified by the prefix *R*.
Default	An administrator configures a static route that identifies the default gateway for packets addressed with a destination network a router does not have in its routing table.

Table 1-17 Routing Algorithms

Distance Vector	Link-State
Periodically exchanges routing tables with neighboring routers.	Exchanges link-state advertisements (LSA) across the network to update routing tables when a change occurs in a link on the network.
Evaluates routes based on a network's distance (how far) and vector (what direction).	Maintains a topological database of the network and builds a shortest path first (SPF) tree to represent the network, with the router at the top.
Distance is expressed in a route cost or metric including hops, administrative cost bandwidth, transmission speed, likeliÏhood of delays, and reliability.	Each time an LSA is received, the router updates and recalculates paths with the SPF algorithm.
A router receives the routing table from a neighbor, updates its routing information, and forwards its routing table with an added hop to neighboring routers.	

Routers from different autonomous systems can communicate with an exterior routing protocol. The routing protocols described in Table 1-18 are interior routing protocols used by routers to exchange routing information within the same autonomous system.

Table 1-18 Routing Protocols

Protocol	Features
Routing Information Protocol (RIP)	Routers exchange complete copies of their routing table with neighbors. Maximum hop count of 15 for routes. RIP uses the hop count to determine the best path across a network. RIP version 2 (RIPv2) is preferred over RIP version 1 because RIPv2 includes subnet mask information in routes, whereas RIP version 1 relies on classful default subnet masks. Therefore, RIPv2 allows VLSM and CIDR.
Enhanced Interior Gateway Routing Protocol (EIGRP)	Uses hop count as well as metrics such as bandwidth and delay to calculate the best path. EIGRP has a maximum hop count of 224. Maintains a routing table, neighbor table, and topology table. Uses advertisements from neighboring routers to build a topology table and then uses the Diffused Update Algorithm (DUAL) to calculate the best path.
Open Shortest Path First (OSPF)	A nonproprietary link-state routing protocol that sends LSA routing updates when a topology change occurs on the network. OSPF supports VLSM, CIDR, and route authentication. It uses the SPF algorithm to calculate the lowest-cost route and maintain an SPF tree.

When you first power on the router, it performs the following tasks in addition to loading Cisco IOS software:

1. The router performs a power-on self-test (POST) to check its hardware.
2. The router loads a bootstrap and initializes the Cisco IOS image from flash, a TFTP server, or read-only memory (ROM). The location of the Cisco IOS image is usually specified in the configuration register. If the router boot field is 0x0, the router boots to ROM. If the boot field is 0x1, the router boots to the IOS.
3. After the IOS image is loaded, the router loads the startup configuration file from nonvolatile random-access memory (NVRAM) to random-access memory (RAM) as the running configuration.

4. If NVRAM has no configuration file, the router searches for a TFTP server with the configuration file. As a last resort, it starts the setup dialog.
5. As soon as the router is up and running, the terminal displays the user EXEC prompt **router>**, and the router is ready for you to configure its interfaces and other parameters.
6. Each time after you configure the router, it is important to execute the command **copy running-config startup-config** to ensure that the router saves the new configuration in NVRAM and will initialize the new configuration when restarted.

Day 11: RIP Configuration

Table 1-19 provides examples of commands available to configure and verify RIPv2.

Table 1-19 Configure and Verify RIPv2

Configuration	Verification
router rip	**ping**
version 2	**show ip route**
network *directly-connected-network*	**show ip protocols**
	debug ip rip
	show running-config

Day 10: CLI Parameters

Table 1-20 provides examples of Cisco IOS editing keys and CLI commands.

Table 1-20 Cisco IOS Editing Keys and Commands

Command/Keystroke	Definition
Tab	Automatically completes a command
Ctrl-P or up arrow	Repeats previously entered commands
Ctrl-A	Moves to the beginning of a command line
Esc-B	Moves back one word
Ctrl-B or left arrowMoves back one character	
Ctrl-E	Moves to the end of the command line
Ctrl-F or right arrow	Moves forward one character
Esc-F	Moves forward one word

Command/Keystroke	Definition
Ctrl-Z	Exits configuration mode
show history	Displays the command buffer
terminal history size *number*	Sets the history buffer size
terminal no editing	Turns off advanced editing
terminal editing	Enables advanced editing

Example 1-2 Router Initial Configuration

```
Router> enable
Router# configure terminal
Router(config)# hostname RouterA
RouterA(config)# banner motd #
Enter TEXT message. End with the character '#'.
Welcome to RouterA
#
RouterA(config)# enable password ciscopass
RouterA(config)# enable secret class
RouterA(config)# line console 0
RouterA(config-line)# password cisco
RouterA(config-line)# login
RouterA(config-line)# exit
RouterA(config)# line vty 0 4
RouterA(config-line)# password cisco
RouterA(config-line)# login
RouterA(config-line)# exit
RouterA(config)# service password-encryption
RouterA(config)# exit
RouterA# copy running-config startup-config
```

Example 1-3 Router Ethernet Interface Configuration

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# interface fa0/0
RouterA(config-if)# ip address 192.168.1.1 255.255.255.0
RouterA(config-if)# description Main Office LAN
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# ip host RouterA 192.168.1.1
RouterA(config)# exit
RouterA# copy running-config startup-config
```

Example 1-4 Router Initial Configuration for SDM

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# ip http server
RouterA(config)# ip http secure-server
RouterA(config)# username cisco privilege 15 password 0 class
RouterA(config)# line vty 0 4
RouterA(config-line)# privilege level 15
RouterA(config-line)# login local
RouterA(config-line)# transport input telent
RouterA(config-line)# transport input telnet ssh
RouterA(config-line)# exit
```

Day 9: Configuration, IOS, and Security

Example 1-5 Configuring a Default Route Using the Exit Interface

```
Router(config)# ip route 0.0.0.0 0.0.0.0 s0
```

Example 1-6 Configuring a Static Route Using the Next-Hop Address

```
Router(config)# ip route 192.168.4.0 255.255.255.0 192.168.3.2
```

Example 1-7 Back up a Configuration to a TFTP Server

```
Router# copy running-config tftp
Address or name of remote host []? 10.0.0.25
Destination filename[router-config]? portland.1
Write file portland.1 to 10.0.0.25 [confirm] y
Writing Portland.1 !!!!!! [ok]
```

Example 1-8 Restore a BackUp Configuration from a TFTP Server

```
Router# copy tftp running-config
Address or name of remote host []? 10.0.0.25
Source filename []? portland.1
Destination filename [running-config]? running-config
Accessing tftp://10.0.0.25/portland.1
!!!!!!!!!!!!!!
752 bytes copied in 8.03 secs
Router#
```

The **show version** command allows you to check the image name of the IOS image on your router. Use the **copy flash tftp** command to copy the IOS image from your router's flash memory to a TFTP server. To restore a backup IOS image from a TFTP server to flash memory, use the command **copy tftp flash**.

Example 1-9 Privileged EXEC Mode Password Security

```
Router> enable
Router# configure terminal
Router(config)# enable password ciscopass
Router(config)# enable secret class
```

Example 1-10 Router Initial Password Configuration

```
Router> enable
Router# configure terminal
Router(config)# line console 0
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exit
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# login
Router(config-line)# exit
```

Example 1-11 Router SSH Configuration for vty 0 4

```
Router> enable
Router# configure terminal
Router(config)# username cisco password class
Router(config)# ip domain-name cisco.com
Router(config)# crypto key generate rsa
[key generation output omitted]
Router(config)# ip ssh ver 2
Router(config)# line vty 0 4
Router(config-line)# login local
Router(config-line)# transport input telnet ssh
```

Day 8: Network Status Verification

Table 1-21 describes common **show** commands you can use to verify network status.

Table 1-21 Common Cisco IOS Software show Commands

Command	Description
show running-config	Displays the running configuration from RAM on the router
show interfaces	Displays information about the router interfaces, including encapsulation, address configuration, and whether the interface is up or down

continues

Table 1-21 Common Cisco IOS Software show Commands *continued*

Command	Description
show arp	Displays any address resolution protocol entries learned by the router
show ip route	Displays routes manually configured or dynamically discovered by the router
show users	Displays any users connected to the router
show version	Displays the version of Cisco IOS software running on the router, the name of the image, and the amount of RAM

Day 7: Wireless Standards

Table 1-22 describes the standards available for wireless connectivity. Table 1-23 describes ad hoc and infrastructure wireless networks.

Table 1-22 IEEE 802.11 Wireless LAN Standards

Standard	Description
802.11	This original standard was released in 1997. It supports a 2-Mbps data rate over the 2.4-GHz frequency. A maximum range is undefined.
802.11a	This amendment was released in 1999. It supports a 54-Mbps data rate over the 5-GHz frequency. The maximum range is estimated at about 50 meters.
802.11b	This amendment was released in 1999. It supports an 11-Mbps data rate over the 2.4-GHz frequency. The maximum range is estimated at about 100 meters.
802.11g	This amendment was released in 2003. It supports a 54-Mbps data rate over the 2.4-GHz frequency. The maximum range is estimated at about 100 meters. 802.11g is backward-compatible with 802.11b.
802.11n	This amendment should be released in 2007. It will support a 540-Mbps data rate over the 2.4-GHz and 5-GHz frequencies. The maximum range is estimated at about 250 meters. 802.11n should be backward-compatible with 802.11a, 802.11b, and 802.11g.

Table 1-23 Wireless LAN Installation Modes

Mode	Network Area	Description
Ad hoc	Independent basic service set (IBSS), in which devices communicate with each other and are not part of a network.	A simple peer-to-peer direct connection among clients to exchange files and data without an access point.
Infrastructure	Basic service set (BSS), in which a group of devices are connected to an access point (AP).	Devices cannot communicate directly. Connectivity is centralized, controlled, and directed by an access point.

Multiple BSS access points can be connected by a distribution system (DS) to form an extended service set (ESS). To create an ESS, each BSS access point's range must overlap by 10 percent and have a common Service Set Identifier (SSID). This allows a client to move through the ESS without a loss of signal.

The following key points define the CSMA/CA process and how a client can reserve a channel on a BSS:

- A device on a BSS asks permission from the AP to communicate in the form of a request to send (RTS).
- If the channel is available, the AP responds with a clear to send (CTS) message.
- The CTS is broadcast to all devices on the BSS so that all devices know that the channel is in use or that a reservation is in place on the channel.
- When the communication is complete, the sending device sends an acknowledgment (ACK) to the AP, saying that the channel can be released. This ACK is also broadcast to all devices on the BSS to indicate that the channel is available.

The following common parameters must be configured on a wireless access point to provide connectivity:

- **Wireless or network mode:** Can be 802.11b, 802.11a, 802.11g, 802.11n, or mixed mode.
- **SSID or network name:** Any device you connect to the WLAN must have the same SSID.
- **Wireless channel:** You can manually configure a channel that does not overlap with nearby BSSs, or you can allow the AP to automatically find the best channel.

Day 6: Wireless Security

Remember the following key points about securing a wireless network:

- It is important to change the default settings such as the SSID and the login to unique settings for your WLAN.
- You can filter network access by MAC address, but users can clone an authorized MAC address to access the network.
- A WEP key has up to 256 bits; however, WPA provides more secure encryption, because it rotates keys. With WPA, both client and AP have the key. WPA2 is an improved version of WPA that uses advanced encryption standard (AES) technology. 802.1x can also provide AP security through user authentication.

Consider the following points when troubleshooting a WLAN:

- **Standards:** The client or AP may be using incompatible standards.
- **Channels:** Overlapping channels may be affecting connectivity.
- **Signal:** A lower-strength signal or outside interference may cause a connection to periodically drop and/or become unreliable.

- **Bandwidth:** An increase in users or high bandwidth utilization may affect network performance.
- **Association:** Make sure that the case-sensitive SSID is correct on clients and the AP and that a client is not connecting to a different BSS.
- **Authentication:** Check that the same keys, encryption protocols, and proper usernames and passwords are in use on the network.

Day 5: Security Threats

The following list describes common social engineering techniques that focus on the user as the weak link:

- **Pretexting:** An attacker masquerades as the help desk or creates a legitimate-sounding scenario to convince the user to reveal sensitive network information.
- **Phishing:** An attacker sends an e-mail posing as a legitimate organization and requests verification of account usernames and passwords.
- **Vishing/phone phishing:** An attacker uses Voice over IP (VoIP) to leave a message with a user that claims to be from a banking service with a callback number.

Attackers can also use software in one of the following forms to gain access to data on a network. Table 1-24 describes options to protect a network from attackers.

- **Virus:** A program that typically is attached to and activated within another legitimate program that then copies itself and uses system and network resources.
- **Worm:** A program that runs independently and uses a network to send copies of itself to all attached hosts.
- **Trojan horse:** A program that looks like a legitimate program to trick the user into installing the software.
- **Denial of service (DoS):** Attackers also use bandwidth and available connections to affect the network's operation. A DoS attack floods a network or server with traffic, preventing any legitimate connections or use.

Table 1-24 Network Protection Options

Method	Installation	Description
Patch	Periodic software updates	Code released after the original release of the software that fixes an issue with the software.
Update	Periodic software updates	Code released after the original release of the software that can patch issues and add functionality to the software. Many operating systems and applications provide configuration options for automatic updates.
Virus protection	Software on workstation or server	Detects and removes viruses, worms, and Trojan horses.

Method	Installation	Description
Spyware protection	Software on workstation or server	Detects and removes spyware and adware.
Spam blocker	Software on workstation or server	Detects and removes undesirable e-mails.
Popup blocker	Software on workstation	Prevents a web page from loading additional windows.
Firewall	Hardware device or software on workstation or server	Filters outgoing and incoming network traffic.

Day 4: Security Applications

A firewall can come packaged as a standalone security appliance, a server-based firewall that installs on a network operating system (NOS), a module that can be installed or is integrated inside an existing router, or a personal firewall that installs on a network host. Firewalls are installed between two networks and can control traffic in the following ways:

- **Filter traffic** based on destination and source IP address or MAC address, block websites based on uniform resource locator (URL) or keywords, and filter traffic based on the type of application used for network transmission.
- Inspect incoming traffic and ensure that each incoming packet is a response to a legitimate outgoing request. This **stateful packet inspection** (SPI) can prevent DoS attacks.
- Firewalls can also provide **network address translation** (NAT) for additional security on an internal network.

Table 1-25 compares the features of Intrusion Detection Systems and Intrusion Prevention Systems.

Table 1-25 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

System	Implementations	Description
IDS	Software (Cisco IOS IPS), hardware, Adaptive Security Appliance (ASA)	Monitors traffic (on one port) and notifies a management station. Can detect only the first malicious transmission, but can reconfigure the router to block future attacks. Used on the network perimeter in front of a firewall to analyze attacks or behind a firewall to detect firewall configuration issues.
IPS	Software (Cisco IOS IPS), hardware, ASA	Traffic passes through the IPS (in one port and out another), which filters suspicious traffic in real time. Can examine the entire data packet from Layer 7 to Layer 2. Usually placed behind a firewall to further examine packets destined for the internal network.

The following three-step process of authentication, authorization, and accounting (AAA) improves network security:

1. **Authentication** requires users to verify their identity with a username and password using a RADIUS or TACACS server.
2. **Authorization** limits access for users based on rights assigned to the user account by the administrator.
3. **Accounting** tracks user network activity and application use.

Day 3: WAN Connections

Table 1-26 describes the features of point-to-point, circuit-switched, and packet-switched WAN connections.

Table 1-26 WAN Connection Types

Connection Type	Description	Example
Point-to-Point Protocol (PPP)	A specific dedicated path through the TSP network that connects two LANs over a large geographic area.	An ISP typically provides leased lines to facilitate a PPP connection.
Circuit-switched	Allows the client to create and close connections over the TSP network. This connection operates like a phone call.	Integrated Services Digital Network (ISDN) or dialup network access.
Packet-switched	A client uses a software-managed virtual circuit over a shared connection.	Frame Relay.

The Cisco default encapsulation for a serial interface is High-Level Data Link Control (HDLC). However, you can change the encapsulation to PPP as a more flexible, nonproprietary encapsulation. In addition, PPP supports authentication in clear-text Password Authentication Protocol (PAP) or encrypted Challenge Handshake Authentication Protocol (CHAP). A router can also use Frame Relay as an encapsulation. Frame Relay virtual circuits use HDLC encapsulation, and each circuit is identified by a data link connection identifier (DLCI).

Example 1-12 Router DTE Serial Interface Configuration Using PPP

```
RouterA> enable
RouterA# configure terminal
RouterA(config)# interface serial 0/0
RouterA(config-if)# description Connection to WAN
RouterA(config-if)# ip address 192.168.2.5 255.255.255.252
RouterA(config-if)# encapsulation ppp
RouterA(config-if)# no shutdown
RouterA(config-if)# exit
RouterA(config)# exit
RouterA# copy running-config startup-config
```

Summary

Treat each detail you review like an old friend. Your attitude is possibly the most important factor for success on the exam. Read with a smile. Your passion for this subject will come through on test day just as clearly as it will come through in a job interview or planning meeting. Good luck on the exam.

Your Notes or Personal Day 1 Outline

Part VIII

Exam and post exam days

Exam Day covers what you will need and should expect at the testing center

Post-Exam Information covers your expectations if you pass or fail the exam

Exam Day

Today is your opportunity to prove that you know how to describe, implement, troubleshoot, and secure a network. 90 minutes and 50 to 60 questions stand between you and your CCENT certification. Use the following information to focus on the process details for the day of your CCENT (ICND1) exam.

What You Need for the Exam

Write the exam location, date, exam time, exam center phone number, and proctor's name on the following lines:

Location: ____

Date: ____

Exam Time (arrive early): ____

Exam Center Phone Number: ____

Proctor's Name: ____

Remember the following items on Exam Day:

- You must have **two forms of ID** that include a photo and signature, such as a driver's license, passport, or military identification.
- The test proctor will take you through the agreement and set up your testing station after you have signed the agreement.
- The test proctor will give you a sheet for scratch paper or a dry erase pad. Do not take these out of the room.
- The testing center will store any personal items while you take the exam. It is best to bring only what you will need.
- You will be monitored during the entire exam.

What You Should Receive After Completion

When you complete the exam, you will see an immediate electronic response as to whether you passed or failed**.** The proctor will give you a certified score report with the following important information:

- Your score report, including the minimum passing score and your score on the exam. The report will also include a breakout displaying your percentage for each general exam topic.
- Identification information that you will need to track your certification. *Do not lose your certified examination score report.*

Summary

Your state of mind is a key factor in your success on the CCENT (ICND1) exam. If you know the details of the curriculum and the details of the exam process, you can begin the exam with confidence and focus. Arrive early to the exam. Bring earplugs in case a testing neighbor has a bad cough or any loud nervous habits. Do not let an extremely difficult or specific question impede your progress. You cannot return to questions on the exam that you have already answered, so answer each question confidently, and keep an eye on the timer.

Post-Exam Information

The accomplishment of signing up for and actually taking the CCENT (ICND1) exam is no small feat. Many network engineers have avoided certification exams for years. The following sections discuss your options after exam day.

Receiving Your Certificate

If you passed the exam, you will receive your official CCENT certificate and wallet card about six weeks (eight weeks internationally) after exam day. Your certificate will be mailed to the address you provided when you registered for the exam.

You will need your examination score report to log in to the certification tracking system and set up a login to check your certification status. If you do not receive your certificate, you have to open a case in the certificate online support located at the following web address:

http://ciscocert.custhelp.com/

When you receive your certificate, you may want to frame it and put it on the wall. A certificate hanging on the wall is much harder to lose than a certificate in a file cabinet or random folder. You never know when an employer or academic institution could request a copy.

Your CCENT is valid for three years. To keep your certificate valid, you must pass the ICND1 exam again, pass an exam bearing the 642 prefix, or advance to the next level of certification before the end of the three-year period.

Determining Career Options

After passing the ICND1 exam, be sure to add your CCENT certification to your resume. Matthew Moran provides the following advice for adding certifications to a resume in his book *The IT Career Builder's Toolkit* (Cisco Press, 2005, ISBN 1587131560):

> *I don't believe you should place your certifications after your name. It is presumptuous to pretend that your latest certification is the equivalent to someone who has spent 4–7 years pursuing a Ph.D. or some other advanced degree. Instead, place your certifications or degrees in a section titled Education and Certifications. A master's degree might be the exception to this rule.*

Moran also discusses good strategies to break into the IT industry after you have earned your CCENT:

> *The most important factor is that you are moving toward a career goal. You might not get the title or job you want right out of school. If you can master those skills at your current position, while simultaneously building your network of contacts that lead to your dream position, you should be satisfied. You must build your career piece by piece. It won't happen all at once.*

Moran also outlines in his book that certifications such as the CCENT are part of an overall professional skill set that you must continually enhance to further your IT career.

Your CCENT certificate proves that you are disciplined enough to commit to a rigorous course of study and follow through with your professional goals. It is unlikely that you will be hired simply because you have a CCENT, but it will place you ahead of other candidates. Even though you have listed the CCENT on your resume, it is important to highlight your networking skills that pertain to the CCENT in your job and skills descriptions on your resume.

Examining Certification Options

Although passing the CCENT (ICND) exam is not easy, it is the starting point for more advanced Cisco certifications, such as the CCNA. When you log in to the online certification tracking tool (use the exam report to do this), be sure to view the certification progress link. This link provides specific information about certifications you can achieve with your CCENT as the base.

The two Cisco associate-level certifications are the Cisco Certified Network Associate (CCNA) and the Cisco Certified Design Associate (CCDA). Both of these certifications require you to pass an additional exam, but with a CCENT under your belt, continued network study and testing should feel more familiar.

If You Fail the Exam

If you fail your first attempt at the CCENT, you have to wait at least five calendar days after the day of the exam to retest. Stay motivated, and sign up to take the exam again within a 30-day period of your first attempt. The score report outlines your weaknesses. Finding a study group or online community can help you with those difficult topics.

If you are familiar with the general concepts, focus on taking practice exams and memorizing the small details that make the exam so difficult. As a Cisco Networking Academy alumnus, you have access to the curriculum, and Packet Tracer provides an excellent simulator for CCENT-level configurations. Consider your first attempt as a formal practice exam and excellent preparation to pass your second attempt.

Summary

Whether or not you display your certificate and update your resume or prepare to conquer the exam on your second attempt, remember to marvel at the innovation and creativity behind each concept you learn. The ability of our society to continually improve communication will keep you learning, discovering, and employed for a lifetime.

Your Notes

Index